symantec™

Norton AntiVirus™ 8.0

For Macintosh®

User's Guide

Norton AntiVirus™ for Macintosh® User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.0

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. LICENSE:

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. SIXTY DAY MONEY BACK GUARANTEE:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER

RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

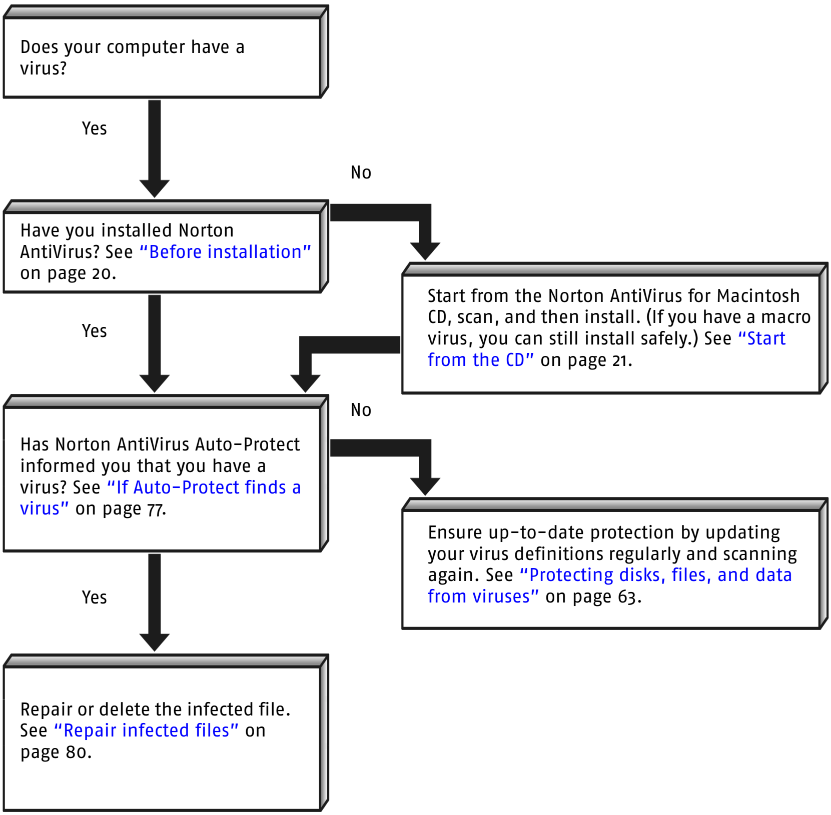
6. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items”, as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation”, as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

What to do if a virus is found



Does your computer have a virus?

Have you installed Norton AntiVirus? See “Before installation” on page 20.

Start from the Norton AntiVirus for Macintosh CD, scan, and then install. (If you have a macro virus, you can still install safely.) See “Start from the CD” on page 21.

Has Norton AntiVirus Auto-Protect informed you that you have a virus? See “If Auto-Protect finds a virus” on page 77.

Ensure up-to-date protection by updating your virus definitions regularly and scanning again. See “Protecting disks, files, and data from viruses” on page 63.

Repair or delete the infected file. See “Repair infected files” on page 80.

Contents

Chapter 3 Norton AntiVirus for Macintosh basics

Chapter 4 Keeping current with LiveUpdate

Chapter 5 Protecting disks, files, and data from viruses

Chapter 6 What to do if a virus is found

Chapter 7 Customizing Norton AntiVirus for Macintosh

About Norton AntiVirus for Macintosh

Norton AntiVirus for Macintosh provides comprehensive virus prevention, detection, and elimination software for your computer. It finds and repairs infected files (files that contain viruses) to keep your data safe and secure. Norton AntiVirus easily updates its *virus definitions* (virus information that lets an anti-virus program recognize and alert you to the presence of a specific virus) over the Internet to stay prepared for the latest threats.

Versions of Norton AntiVirus for both Mac OS 8.1-9.x and Mac OS X v10.1 are included on the CD.

What's new in Norton AntiVirus for Macintosh

Norton AntiVirus for Macintosh protects your computer with more flexible configuration and control features, automatic repair of infected files, and the ability to schedule scans when you want.

- Auto-Protect: This version includes the first OS X v10.1-compatible version providing constant monitoring of your computer.
- SafeZones: Ensures that your entire computer is protected from viruses by designating it a Universal SafeZone and scanning all files saved to disk.
- Scheduler: Lets you designate when you want Norton AntiVirus to scan your computer and schedule when you want LiveUpdate to run.

How viruses work

A *computer virus* is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files and, when activated, may damage files, cause erratic system behavior, or display messages.

Computer viruses infect *System files* (files stored in the System folder that the Macintosh computer uses to start up) and documents created by programs with macro capabilities. Mac OS System files include *system extensions* (programs that load into memory when a Macintosh computer is started), and programs like those in Microsoft Office.

Some system viruses are programmed specifically to corrupt programs, delete files, or erase your disk. Many of the currently known Macintosh viruses; however, are not designed to do any damage. They replicate themselves and may display messages. Nevertheless, bugs within the viruses may cause your system to behave erratically or crash unexpectedly.

Macro viruses spread quickly

Macros are simple programs that are used to do things such as automate repetitive tasks in a document or make calculations in a spreadsheet. Macros are written in files created by such programs as Microsoft Word and Microsoft Excel.

Macro viruses are malicious macro programs that are designed to replicate themselves from file to file and can often destroy or change data. Macro viruses can be transferred across platforms and spread whenever you open an infected file.

Trojan horses hide their true purposes

Trojan horses are programs that appear to serve some useful purpose or provide entertainment, which encourages you to run them. But the program also serves a covert purpose, which may be to damage files or place a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus. Because Trojan horses are not viruses, files that contain them cannot be repaired. To ensure the safety of your computer, Norton AntiVirus detects Trojan horses so you can delete them from your computer.

Worms take up space

Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk. They search for specific types of files on a hard disk and try to damage or destroy those files. Other worms replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer. Like Trojan horses, worms are not viruses and therefore cannot be repaired. They must be deleted from your computer.

How viruses spread

A virus is inactive until you launch an infected program, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any program you run, including network programs (if you can make changes to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected program is running. Turning off your computer or exiting the program removes the virus from memory, but does not remove the virus from the infected file or disk. That is, if the virus resides in an operating system file, the virus activates the next time you start your computer from the infected disk. If the virus resides in a program, the virus activates the next time you run the program.

To prevent virus-infected programs from getting onto your computer, scan files with Norton AntiVirus before you copy or run them. This includes programs you *download* (transfer from one computer system to another through a modem or network) from news groups or Internet Web sites and any email attachments that you receive.

Macintosh computers that are attached to multiplatform *networks* (sets of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users) can potentially be affected by Windows-based viruses. If you store Macintosh files on network servers accessible by Windows-based computers, those files could potentially be attacked by Windows viruses or worms programmed to damage files. Macintosh anti-virus programs such as Norton AntiVirus for Macintosh can’t protect Macintosh computers against these kinds of cross-platform attacks. Users on networks should make sure that their network and PC computers are protected by network-wide anti-virus solutions.

How Norton AntiVirus for Macintosh works

Norton AntiVirus monitors your computer for known and unknown viruses. A *known virus* is one that can be detected and identified by name. An *unknown virus* is one for which Norton AntiVirus does not yet have a definition.

Norton AntiVirus protects your computer from both types of viruses, using virus definitions to detect known viruses and Bloodhound technology to detect unknown viruses. Virus definitions and Bloodhound technology are used during scheduled scans and manual scans, and are used by Auto-Protect to constantly monitor your computer.

The virus definition service stops known viruses

See "Look up virus definitions on the Symantec Web site" on page 85.

The *virus definition service* consists of files that Norton AntiVirus uses to recognize viruses and intercept their activity. You can look up virus names in Norton AntiVirus and access an encyclopedia of virus descriptions on the Symantec Web site.

Bloodhound technology stops unknown viruses

Bloodhound is the Norton AntiVirus scanning technology for detecting new and unknown viruses. It detects viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file.

Auto-Protect keeps you safe

Norton AntiVirus Auto-Protect loads into memory when your computer starts up, providing constant protection while you work. It eliminates viruses and Trojan horses, including macro viruses, and repairs damaged files. It monitors your computer for any unusual symptoms that may indicate an active virus. It also checks for viruses every time you use software programs on your computer, insert floppy disks or other removable media, use the Internet, or use document files that you receive or create.

SafeZones isolate potentially damaging files

You risk infecting your computer every time you download or receive a file from the Internet or email or copy files from any other source.

SafeZones are special locations on your computer that are protected by Norton AntiVirus Auto-Protect. To prevent virus infection, Auto-Protect scans any file for viruses that is copied or downloaded to an area designated as a SafeZone. The cursor changes to a special Auto-Protect cursor while files are scanned.

See "About SafeZone Preferences" on page 93.

In Mac OS 8.1-9.X, when you perform a standard installation, part of your computer is set up as a Custom SafeZone. You can designate any folder as a SafeZone. To configure your SafeZone settings to protect your entire computer, including email folders, Internet folders, and network volumes, establish a Universal SafeZone.

In Mac OS X v10.1, although you cannot designate custom SafeZones, all files written to disk, including all files downloaded or received via email, are scanned by Norton AntiVirus.

How to maintain protection

When Norton AntiVirus is installed, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer from an infected disk or when you run an infected program. There are several things you can do to avoid viruses and to recover quickly should a virus strike.

Avoid viruses

It is important that you practice regular file maintenance and that you keep Norton AntiVirus up-to-date.

To avoid viruses:

- Manually scan removable media.
- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (http://securityresponse.symantec.com) where there is extensive, frequently updated information on viruses and virus protection.

See "Keeping current with LiveUpdate" on page 49.

- Use LiveUpdate regularly to update your programs and virus definition service files.
- Keep Norton AntiVirus Auto-Protect turned on at all times to prevent viruses from infecting your computer.

See "Scan disks, folders, and files" on page 63.

- If Norton AntiVirus Auto-Protect is not turned on, scan removable media before you use them. In Mac OS X v10.1, always scan removable media before you use them.

See "Add scheduled Norton AntiVirus scans" on page 69.

- Schedule scans to occur automatically.

Prepare for emergencies

It is also important that you are prepared in case your computer is infected by a virus. To prepare for emergencies back up files regularly and keep more than just the most recent backup.

If you can't start from the CD

Some third-party CD drives cannot start a computer from a CD. As an alternative to the CD, set up another disk, a partition on a disk, or a removable disk such as a Zip or SuperDisk drive as a *startup disk* (a disk that contains the system files necessary to start your computer).

To set up another drive as a startup disk

1. Install your Macintosh OS System software to the designated disk.
2. Install Norton AntiVirus onto this new startup disk.
   Restart from that disk to run Norton AntiVirus in an emergency.

To restart your computer with the new startup disk in Mac OS 8.1-9.x

1. On the Apple menu, click **Control Panels > Startup Disk**.
2. Double-click **Norton AntiVirus for Macintosh CD** to make it your startup disk.
3. Close the Startup Disk Control Panel.
4. On the Special menu, click **Restart**.
   Your computer will start up from the designated volume.

To restart your computer with the new startup disk in Mac OS X v10.1

1. On the Apple menu, click **System Preferences**.
2. Double-click **Startup Disk**.
3. Click **Norton AntiVirus for Macintosh CD**.
4. Click **Restart**.
5. In the window that comes up, click **Save and Restart**.

See "Service and support solutions" on page 133.

The System software included on the Norton AntiVirus for Macintosh CD might not be sufficient to start newer Macintosh models issued after the release of this version of Norton AntiVirus for Macintosh. To find out if a newer CD is available, contact Symantec Customer Service.

Installing Norton AntiVirus for Macintosh

2

Restart from the CD and scan for viruses before installing Norton AntiVirus for Macintosh.

Files from previous versions of Norton AntiVirus for Macintosh and Symantec AntiVirus for Macintosh (SAM) are deleted when you install Norton AntiVirus to the same location.

System requirements

The system requirements are different, depending on whether you are installing Norton AntiVirus for Mac OS 8.1-9.x or Norton AntiVirus for Mac OS X v10.1.

Mac OS 8.1–9.x

- Macintosh OS 8.1-9.x (8.5 or later for Control Strip functionality)
- Macintosh PowerPC processor
- 24 MB of RAM
- 10 MB of available hard disk space for installation
- 3 MB of available hard disk space
- Internet connection
- CD-ROM or DVD-ROM drive

Mac OS X v10.1

Norton AntiVirus for Macintosh does not support Mac OS X versions 10.0-10.0.4. If you want to install Norton AntiVirus for Macintosh on Mac OS X, you must upgrade to Mac OS X v10.1.

- Macintosh OS X (v10.1 or later)
- G3 or G4 processor
- 128 MB of RAM
- 10 MB of available hard disk space for installation
- Internet connection
- CD-ROM or DVD-ROM drive

Before installation

Restart your computer from the Norton AntiVirus for Macintosh CD and scan all mounted volumes for viruses before installing. Starting from the CD ensures that no viruses are in memory and that no system extensions cause conflicts during installation. Scanning all mounted volumes ensures that no viruses are on the disks.

Read the Read Me file

The Read Me file contains a summary of what's new and changed in Norton AntiVirus for Macintosh, along with condensed versions of key procedures and technical tips. In addition, see the Read Me file for late-breaking information and installation troubleshooting tips.

To read the file

1. Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.
2. Open the folder for the version of Norton AntiVirus you are installing.
3. Double-click **Norton AntiVirus Read Me**.

Start from the CD

Start from the Norton AntiVirus for Macintosh CD to scan your disk before you install if you suspect that it is infected with a virus.

To start your computer from the Norton AntiVirus for Macintosh CD

1. Insert your Norton AntiVirus for Macintosh CD into the CD-ROM drive.
2. Restart your computer from the Norton AntiVirus for Macintosh CD by using one of the following methods:
   - On the Special menu (in Mac OS 8.1-9.x) or the Apple menu (in Mac OS X v10.1), click **Restart**, while pressing **C**.
   - On a Macintosh computer with a third-party or external CD-ROM drive, on the Apple menu, click **Control Panels > Startup Disk**, and double-click **Norton AntiVirus for Macintosh CD** to make it your startup disk. Close the Startup Disk Control Panel. On the Special menu, click **Restart**.
     You can tell that your computer has restarted from the CD because the Norton AntiVirus for Macintosh pattern appears in the background of the desktop.
   - In Mac OS X v10.1 on the Apple menu, click **System Preferences**, and click the **Startup Disk** icon. Double-click **Norton AntiVirus for Macintosh CD** to make it your startup disk. Click **Restart**, then in the window that comes up, click **Save and Restart.**
3. If the CD window doesn’t open automatically, double-click the CD icon to open it.

Scan for viruses

To make sure that no viruses are already on your computer, scan it before installing Norton AntiVirus.

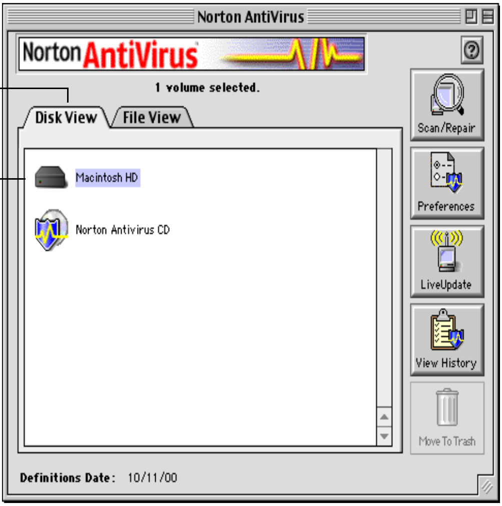
To scan for viruses

See "Start from the CD" on page 21.

1 Start your computer using the Norton AntiVirus for Macintosh CD.

2 In the CD window, double-click **Norton AntiVirus**.
If you have already downloaded a more recent virus definitions file than the one currently on the Norton AntiVirus for Macintosh CD, use it to scan. Press **Option** when you open Norton AntiVirus, then select the newer virus definitions file.

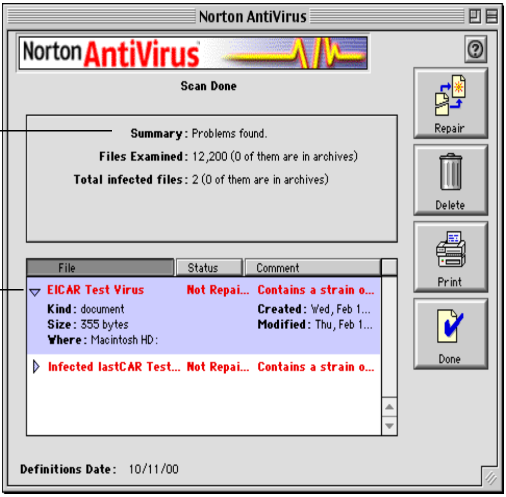
3 In the Norton AntiVirus main window, on the Disk View tab, select the disk to scan.



Click the Disk View tab if it is not in front

Select the item that you want Norton AntiVirus to scan

4 Click **Scan/Repair**.
Norton AntiVirus scans the selected disk. If a virus is found during the scan, Norton AntiVirus repairs it automatically. When the scan is complete, the results appear in the scan window.



Scan Done

Summary: Problems found.
Files Examined: 12,200 (0 of them are in archives)
Total infected files: 2 (0 of them are in archives)

▽ EICAR Test Virus | Not Repai... | Contains a strain o...
Kind: document | **Created:** Wed, Feb 1...
Size: 355 bytes | **Modified:** Thu, Feb 1...
Where: Macintosh HD:
▷ Infected lastCAR Test... | Not Repai... | Contains a strain o...

Definitions Date: 10/11/00

See "If a virus is found while scanning" on page 79.

5 Click **Done**.

6 On the File menu, click **Quit**.

Installation

Install Norton AntiVirus from the Norton AntiVirus for Macintosh CD.

See "Read the Read Me file" on page 20.

The Installer for each version of Mac OS for Norton AntiVirus is contained in its own folder on the CD, along with installation instructions and a Read Me file specific to that version.

You need to know your Mac OS administrator password before you start the installation process. You are prompted for your password and cannot install without it. To get instructions on how to retrieve your password access your Mac Help.

Install Norton AntiVirus for Mac OS 8.1–9.x

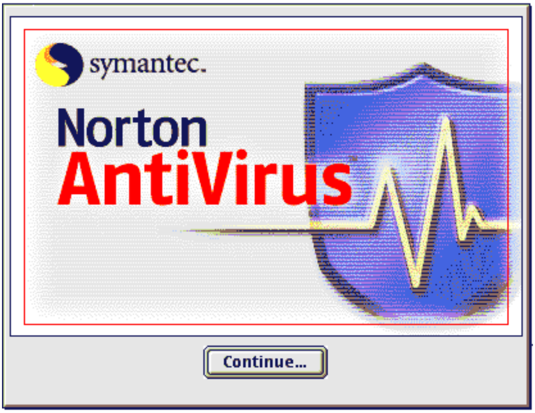
After you have restarted your computer from the CD and scanned your disk to ensure that it is virus-free, you are ready to install Norton AntiVirus for Macintosh. You can use Easy Install for a full installation, or Custom Install to install selected components. Both types of installations have the same first few steps.

To install Norton AntiVirus for Macintosh OS 8.1–9.x

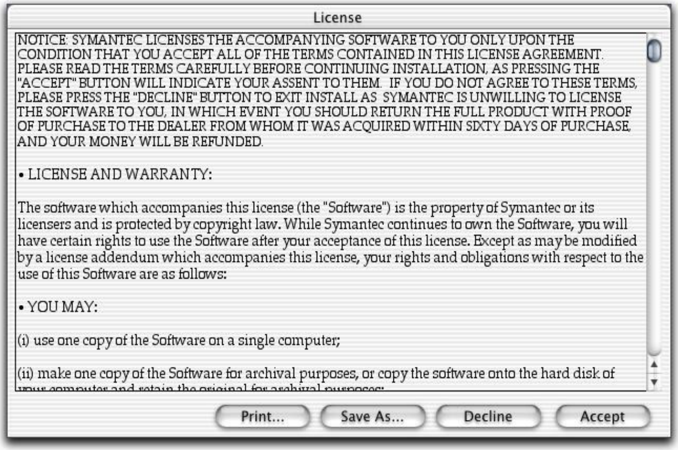
1 Insert the Norton AntiVirus for Macintosh CD into the CD-ROM drive. If the CD window doesn't open automatically, double-click the CD icon to open it.

2 In the CD window, open the **Install for OS 8.1-9.x** folder.

3 Double-click **Norton AntiVirus Installer**.



4 In the Norton AntiVirus welcome window, click **Continue**.



NOTICE: SYMANTEC LICENSES THE ACCOMPANYING SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE CONTINUING INSTALLATION, AS PRESSING THE "ACCEPT" BUTTON WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, PLEASE PRESS THE "DECLINE" BUTTON TO EXIT INSTALL AS SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

• LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensers and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

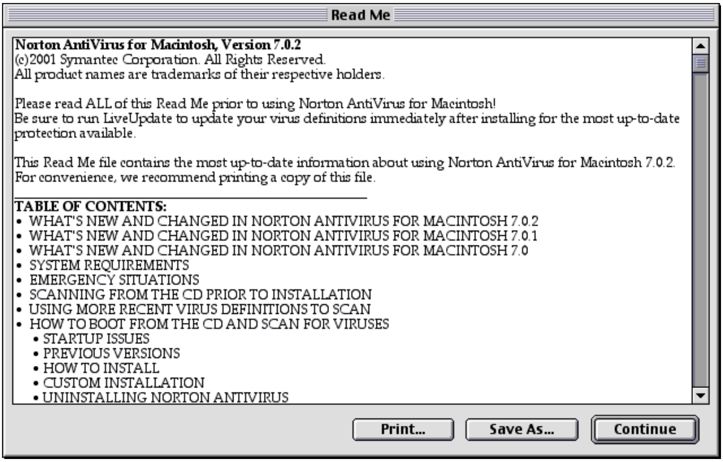
• YOU MAY:

(i) use one copy of the Software on a single computer;

(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

5 Click **Accept** to accept the License and Warranty Agreement.

If you decline, the installation is cancelled.



Norton AntiVirus for Macintosh, Version 7.0.2
(c)2001 Symantec Corporation. All Rights Reserved.
All product names are trademarks of their respective holders.

Please read ALL of this Read Me prior to using Norton AntiVirus for Macintosh! Be sure to run LiveUpdate to update your virus definitions immediately after installing for the most up-to-date protection available.

This Read Me file contains the most up-to-date information about using Norton AntiVirus for Macintosh 7.0.2. For convenience, we recommend printing a copy of this file.

TABLE OF CONTENTS:

- WHAT'S NEW AND CHANGED IN NORTON ANTIVIRUS FOR MACINTOSH 7.0.2
- WHAT'S NEW AND CHANGED IN NORTON ANTIVIRUS FOR MACINTOSH 7.0.1
- WHAT'S NEW AND CHANGED IN NORTON ANTIVIRUS FOR MACINTOSH 7.0
- SYSTEM REQUIREMENTS
- EMERGENCY SITUATIONS
- SCANNING FROM THE CD PRIOR TO INSTALLATION
- USING MORE RECENT VIRUS DEFINITIONS TO SCAN
- HOW TO BOOT FROM THE CD AND SCAN FOR VIRUSES
  - STARTUP ISSUES
  - PREVIOUS VERSIONS
  - HOW TO INSTALL
  - CUSTOM INSTALLATION
  - UNINSTALLING NORTON ANTIVIRUS

6 Scroll through the Read Me text file, then click **Continue**.

7 In the main Installer window, do one of the following:

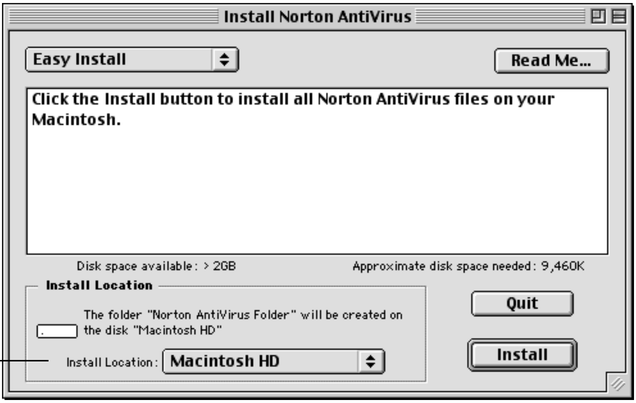
- For a full installation, click **Easy Install**.
  Continue with the steps listed in “Easy Install” on page 26.
- To select individual components, click **Custom Install**.
  Continue with the steps listed in “Custom Install” on page 27.

Easy Install

Easy Install installs all components of Norton AntiVirus.

To complete an Easy Install

1 In the Install Norton AntiVirus window, under Install Location, confirm or specify a destination folder to which to install.



Click the Install button to install all Norton AntiVirus files on your Macintosh.

Disk space available : > 2GB

Approximate disk space needed : 9,460K

The folder "Norton AntiVirus Folder" will be created on the disk "Macintosh HD"

Install Location : Macintosh HD

Specify the destination for the software

2 If you have multiple partitions on your Macintosh and have a System folder in each one, you are prompted to select a System folder for installation.

See "Keeping current with LiveUpdate" on page 49.

A subscription notice appears describing the subscription to virus definitions. Updates are made available monthly, or more frequently when necessary. You can obtain regular virus definitions updates manually or on a customized schedule using LiveUpdate.

3 After you have read the subscription notice, click **OK**.

See "Select a protection level during installation" on page 28.

4 Select or confirm the Virus Scanning Preferences.

5 Click **Set Preferences and Continue**.
If you had a previous version of Norton AntiVirus over which you are installing, a message appears telling you the older version was moved to the Trash.

6 Follow the on-screen instructions to complete the installation.

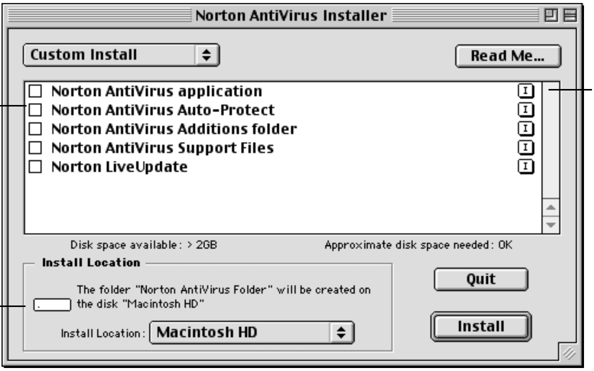
7 Click **Quit** when installation has completed.
For instructions on restarting your computer from the hard disk, see "Restart your computer" on page 31.

Custom Install

Use Custom Install to select individual components of Norton AntiVirus to install.

To complete a Custom Install

1 Check the Norton AntiVirus components that you want to install.



□ Norton AntiVirus application
□ Norton AntiVirus Auto-Protect
□ Norton AntiVirus Additions folder
□ Norton AntiVirus Support Files
□ Norton LiveUpdate

Disk space available : > 2GB

Approximate disk space needed : 0K

Install Location

The folder "Norton AntiVirus Folder" will be created on the disk "Macintosh HD"

Install Location : Macintosh HD

Available components

Destination for the software

Click to see a description of the component

These are the available components to install:

Norton AntiVirus application	Installs Norton AntiVirus and any needed support files
Norton AntiVirus Auto-Protect	Installs the Auto-Protect extension in the Extensions folder
Norton AntiVirus Additions Folder	Installs the Additions folder in the Extensions folder
Norton AntiVirus Support files	Installs the contextual menu, small scanner, and the Auto-Protect Control Strip module
Norton LiveUpdate	Installs LiveUpdate for product and virus definition updates

2 Confirm or specify the Install Location.

3 Click **Install**.

A subscription notice appears describing the subscription to virus definitions. Updates are made available monthly, or more frequently when necessary. You can obtain regular virus definitions updates manually or on a customized schedule using LiveUpdate.

See "Keeping current with LiveUpdate" on page 49.

4 After you have read the subscription notice, click **OK**.

See "Select a protection level during installation" on page 28.

5 Select or confirm the Virus Scanning Preferences.

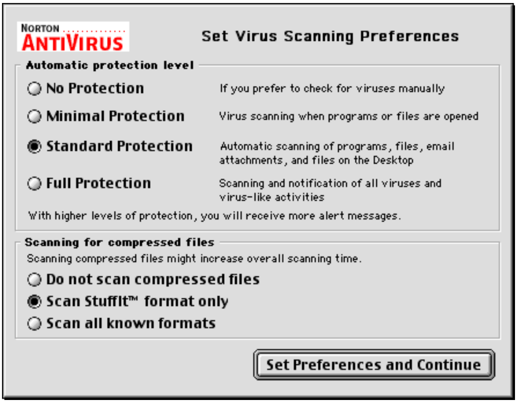
6 Click **Set Preferences and Continue**.

7 Follow the on-screen instructions to complete the installation.

8 Click **Quit** when installation has completed.
For instructions on restarting your computer from your startup disk, see "Restart your computer" on page 31.

Select a protection level during installation

During the installation of Norton AntiVirus for Mac OS 8.1-9.x, select a level of virus protection that matches your computing needs. These levels are combinations of more detailed custom preferences.



Norton AntiVirus

Set Virus Scanning Preferences

Automatic protection level

○ No Protection — If you prefer to check for viruses manually

○ Minimal Protection — Virus scanning when programs or files are opened

● Standard Protection — Automatic scanning of programs, files, email attachments, and files on the Desktop

○ Full Protection — Scanning and notification of all viruses and virus-like activities

With higher levels of protection, you will receive more alert messages.

Scanning for compressed files

Scanning compressed files might increase overall scanning time.

○ Do not scan compressed files

● Scan StuffIt™ format only

○ Scan all known formats

Select from the following protection levels:

No Protection	Auto-Protect is turned off. You have no automatic virus protection with this setting. You can scan for viruses manually, or use the contextual menu to scan selected items, or use the control-strip feature to turn Auto-Protect on.
Minimal Protection	Auto-Protect is turned on, but only scans files being opened or created, and Internet file downloads.
Standard Protection	Provides comprehensive protection that monitors Internet activity, installations, and file exchanges, and provides warnings of common virus-like activities.
Full Protection	All of your computing activities are monitored for virus activities. Use this setting if you use File Sharing on your computer, or your computer is exposed to viruses.

The Compression Scanning options let you select the types of *compressed files* (files that have been compressed such that the resulting data occupies less physical space on the disk) Norton AntiVirus will scan. Because compressed files take longer to scan, you might want to adjust these settings.

To change settings later, see "To set Compression Preferences in Mac OS 8.1-9.x" on page 105.

Install Norton AntiVirus for Mac OS X v10.1

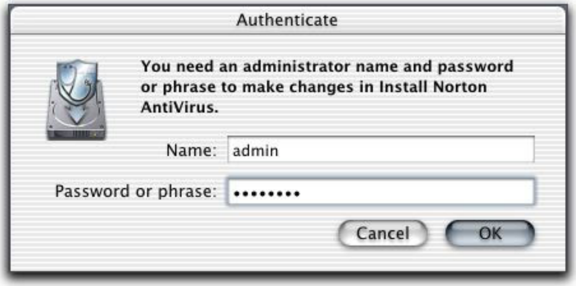
You must start your computer in Mac OS X v10.1 and know your administrator password in order to install Norton AntiVirus for Mac OS X v10.1. If you do not know if your logon has administrator privileges, or you need to change your administrator password, you can do so in System Preferences.

To check your logon type

1. In Mac OS X v10.1, open **System Preferences**.
2. Click **Users**.
   Your logon name and type are listed.

To install Norton AntiVirus for Mac OS X v10.1

1. Insert the Norton AntiVirus for Macintosh CD into the CD-ROM drive.
   If the CD window doesn't open automatically, double-click the CD icon to open it.
2. In the CD window, open the **Install for OS X** folder.
3. Double-click **Install Norton AntiVirus**.



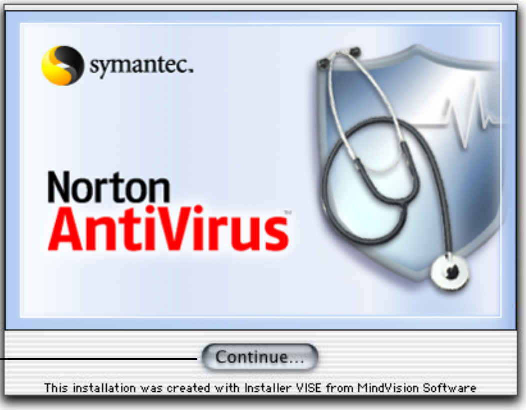
Authenticate

You need an administrator name and password or phrase to make changes in Install Norton AntiVirus.

Name: admin

Password or phrase: ••••••••

4 Enter your administrator password.



This installation was created with Installer VISE from MindVision Software

Click to continue

5 Click **Install**.

A subscription notice appears describing the subscription to virus definitions. Updates are made available monthly, or more frequently when necessary. You can obtain regular virus definitions updates using LiveUpdate.

See "Keeping current with LiveUpdate" on page 49.

6 After you have read the subscription notice, click **OK**.

7 Click **OK**.

8 Follow the on-screen instructions to complete the installation.

9 Click **Quit** when installation has completed.

After installation

Now that you've installed Norton AntiVirus, you have the following options:

More information	Activity
See "Restart your computer" on page 31.	Restart your computer from your usual startup disk.
See "Register Norton AntiVirus" on page 32.	Register your software to take advantage of your virus definitions subscription.
See "Read Late Breaking News" on page 33.	Check for late-breaking news about your new software. Use the Internet link installed in the Norton Solutions folder.

More information	Activity
See "Explore the CD" on page 34.	Get information about additional features and programs included on the CD.
See "Keeping current with LiveUpdate" on page 49.	Use LiveUpdate to get the latest virus protection. You can also download new virus definitions from the Symantec Security Response Web site, http://securityresponse.symantec.com.
See "Scan disks, folders, and files" on page 63.	Scan all of your disks to make sure they are virus-free.
See "About program updates" on page 49.	Learn more about virus prevention.
See "About Custom Preferences" on page 90.	Customize the installed settings for Norton AntiVirus.

Restart your computer

You need to restart your computer from the startup disk after installing Norton AntiVirus. If you have installed while started from the CD, you must first restore your computer's settings.

To restore your computer's settings

1. Click **Control Panels** > **Startup Disk**.
2. Click your disk to make it the startup disk.
3. Close the Control Panel.
4. On the Special menu, click **Restart**.

If you can't eject the CD

If you have trouble ejecting the CD after you restart your computer, try one of the following:

- Press the CD-ROM drive's eject button when your Macintosh restart chime sounds.
- On newer Macintosh computers with a slot-loading CD-ROM drive, press the mouse button while starting up to eject the CD.

When you install Norton AntiVirus with the Standard Protection, you are protected from most viruses after you restart. With this level of protection, in Mac OS 8.1-9.x, Norton AntiVirus Auto-Protect loads when you restart and actively protects your computer unless you turn Auto-Protect off.

Register Norton AntiVirus

Using your existing Internet connection, you can register Norton AntiVirus for Macintosh via the *Internet* (the global network of computers).

If you are running Macintosh OS 8.5 or later, an icon in the Norton AntiVirus for Macintosh folder lets you launch your browser and connect to the Symantec software registration page. If you are running an earlier version of Macintosh OS, point your *browser* (software application that makes navigating the Internet easy by providing a graphical user interface) to the Symantec Web site.

To register Norton AntiVirus via the Internet

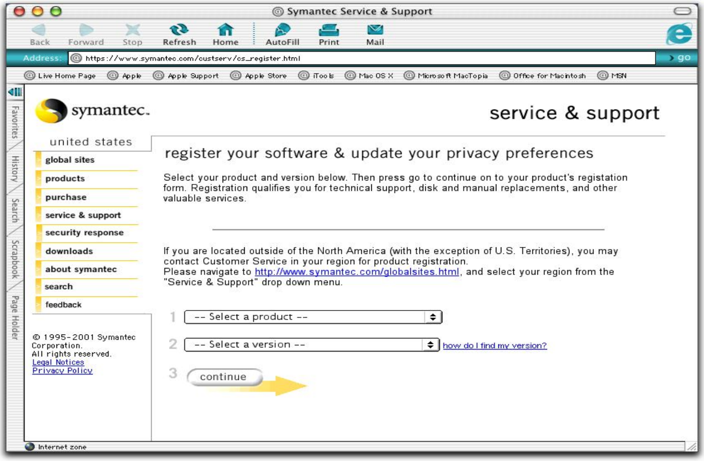
1 Connect to the Internet.
If you use America Online (AOL) to connect to the Internet, see "To connect to the Symantec Web site via AOL" on page 34.

2 In the Norton AntiVirus for Macintosh folder, double-click **Register Your Software**.

Your default Internet browser displays the Symantec Service & Support registration page.

3 If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Service & Support page:
www.symantec.com/custserv/cs_register.html

4 On the Service & Support page, select Norton AntiVirus for Macintosh as the product, select the correct version of the product, then click **Go**.



register your software & update your privacy preferences

Select your product and version below. Then press go to continue on to your product's registation form. Registration qualifies you for technical support, disk and manual replacements, and other valuable services.

If you are located outside of the North America (with the exception of U.S. Territories), you may contact Customer Service in your region for product registration.
Please navigate to http://www.symantec.com/globalsites.html, and select your region from the "Service & Support" drop down menu.

1 -- Select a product --

2 -- Select a version -- how do I find my version?

3 continue

© 1995-2001 Symantec Corporation.
All rights reserved.
Legal Notices
Privacy Policy

5 On the registration page for Norton AntiVirus for Macintosh, type all of the required information.

6 Click **Submit Registration**.

Read Late Breaking News

Norton AntiVirus installs a Late Breaking News link. This link lets you see the latest information for your installed software.

To read Late Breaking News

1 Connect to the Internet.
If you use America Online (AOL) to connect to the Internet, see "To connect to the Symantec Web site via AOL" on page 34.

2 In the Norton AntiVirus for Macintosh folder, double-click **Late Breaking News**.

Your default Internet browser displays the Symantec Late Breaking News Web page for your product.

3 If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Web page:
www.symantec.com/product/home-mac.html

If you connect to the Internet through America Online

If you use America Online (AOL) as your Internet Service Provider (ISP), you must connect to AOL before you go to the Symantec software registration page or view Late Breaking News.

To connect to the Symantec Web site via AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Move the AOL browser and any other open AOL windows out of the way.
4. In the Norton AntiVirus window, do one of the following:
   - Double-click **Register Your Software**.
     Continue with the registration procedure. See "Register Norton AntiVirus" on page 32.
   - Double-click **Late Breaking News**.
     Continue with the procedure for reading the news. See "Read Late Breaking News" on page 33.
5. Disconnect from AOL.

Explore the CD

In addition to the Norton AntiVirus for Macintosh installer folders and program software, there are several other items on the CD:

SimpleText program	Lets you read the Read Me file in Mac OS 8.1-9.x.
Documentation folder	Contains this User's Guide in PDF format and installation files for Adobe Acrobat Reader.
System folder	Lets you restart from the CD to run Norton AntiVirus before you install, or any time you need to scan the disk containing your active System folder.

Norton Solutions folder	Contains the Norton AntiVirus for Mac OS 8.1-9.x program and related files. It also contains the LiveUpdate files. Use LiveUpdate to update your installed virus program files and obtain the latest virus definitions.

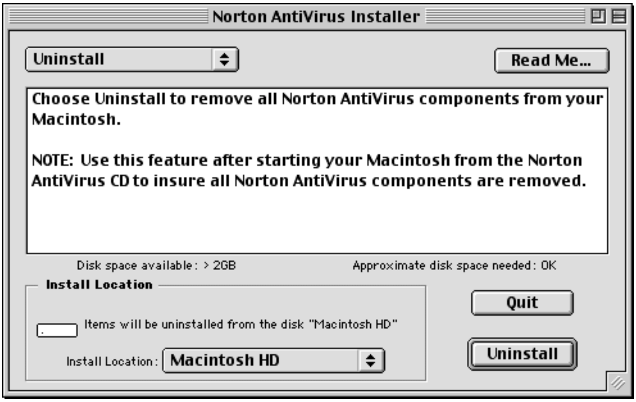
If you need to uninstall Norton AntiVirus

If you need to remove Norton AntiVirus from your computer, use the Norton AntiVirus Installer. The process will be faster if all other programs are closed before you uninstall Norton AntiVirus.

To uninstall Norton AntiVirus for Mac OS 8.1–9.x

1. Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.
   If the CD window doesn't open automatically, double-click the CD icon.
2. In the CD window, open the **Install for OS 8.1-9.x** folder.
3. Double-click **Norton AntiVirus Installer**.
4. Click **Continue** to progress through the information screens.
5. Click **Accept** to accept the License and Warranty Agreement.
   If you decline, the installation is cancelled.
6. In the drop-down list, click **Uninstall**.
7. Select the disk from which to uninstall Norton AntiVirus.

8 Click **Uninstall**.



Choose Uninstall to remove all Norton AntiVirus components from your Macintosh.

NOTE: Use this feature after starting your Macintosh from the Norton AntiVirus CD to insure all Norton AntiVirus components are removed.

Disk space available: > 2GB

Approximate disk space needed: 0K

Install Location

Items will be uninstalled from the disk "Macintosh HD"

Install Location: Macintosh HD

Norton AntiVirus removes its files from your system.

Your computer must be started in Mac OS X v10.1 to uninstall Norton AntiVirus for Mac OS X v10.1.

To uninstall Norton AntiVirus for Mac OS X v10.1

1 Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.

2 In the CD window, open the **Install for OS X** folder.

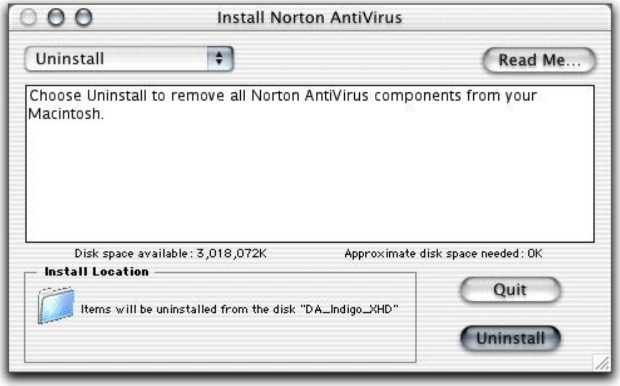
3 Double-click **Install Norton AntiVirus**.

4 In the Authenticate dialog box, type your administrator password.

5 Click **Continue** to progress through the information screens.

6 Click **Accept** to accept the License and Warranty Agreement.
If you decline, the installation is cancelled.

7 In the drop-down list, click **Uninstall**.



Choose Uninstall to remove all Norton AntiVirus components from your Macintosh.

Disk space available: 3,018,072K Approximate disk space needed: 0K

Install Location

Items will be uninstalled from the disk "DA_Indigo_XHD"

8 Select the disk from which to uninstall Norton AntiVirus.

9 Click **Uninstall**.
Norton AntiVirus removes its files from your system.

Norton AntiVirus for Macintosh basics

3

Norton AntiVirus basics include general information about how to work with Norton AntiVirus and how to access more information about Norton AntiVirus.

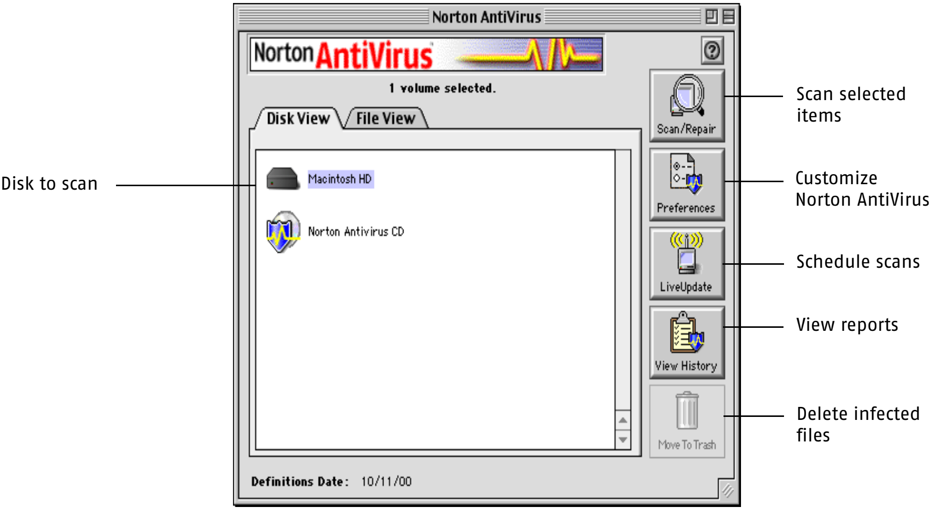
How to start and exit Norton AntiVirus

You don’t have to start the Norton AntiVirus program to be protected from viruses if you have Auto-Protect running. You do have to start Norton AntiVirus when you want to:

- Run manual scans of your computer.
- Schedule Norton AntiVirus to run unattended scans.
- Customize virus protection options.
- Repair infections found by Auto-Protect when files are opened or programs are launched and Auto-Repair is turned off.

To start Norton AntiVirus

1. Open the **Norton Solutions** folder.
2. Double-click **Norton AntiVirus**.



To exit Norton AntiVirus in Mac OS 8.1-9.x

❖ Do one of the following:

- On the File menu, click **Quit**.
- Press **Command-Q**.

To exit Norton AntiVirus in Mac OS X v10.1

❖ Do one of the following:

- On the Norton AntiVirus menu, click **Quit Norton AntiVirus**.
- Press **Command-Q**.

Enable and disable Norton AntiVirus Auto-Protect

Norton AntiVirus Auto-Protect guards against viruses as soon as your computer starts. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. In Mac OS 8.1-9.x, when a virus or *virus-like activity* (an event that could be the work of a virus) is detected, Auto-Protect alerts you.

You don't need to run Norton AntiVirus regularly as long as Auto-Protect is active. Auto-Protect interception prevents viruses from moving to your disk, and in Mac OS 8.1-9.x, you can use the contextual menu to scan a specific volume, file, or folder.

If you need to disable Auto-Protect temporarily

Auto-Protect senses when you're installing software in Mac OS 8.1-9.x, so that it doesn't interfere with installation. You can disable it, but it is not recommended.

To disable Auto-Protect temporarily in Mac OS 8.1-9.x

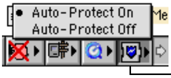
1. Start Norton AntiVirus.
2. On the Preferences menu, click **Turn Auto-Protect Off**.

To disable Auto-Protect temporarily in Mac OS X v10.1

1. Start Norton AntiVirus.
2. In the main window, click **Preferences**.
3. Click **Auto-Protect**.
4. Set Automatic Scanning to **Off**.

Turn Auto-Protect on or off from the Control Strip in Mac OS 8.1-9.x

Norton AntiVirus installs a Control Strip module so you can turn Auto-Protect on or off without opening the Control Panel or the Norton AntiVirus program.



Turn Auto-Protect on or off

Auto-Protect Control Strip icon

To enable the Control Strip

1. On the Apple menu, click **Control Panels**.
2. Click **Control Strip**.
3. Make sure that Show Control Strip is selected, or that a Show/Hide Control Strip hot key is defined.

To turn Auto-Protect on or off from the Control Strip

1. Open the Control Strip.
2. Click the **Auto-Protect** Control Strip module.
3. On the pop-up menu, select one of the following:
   - Auto-Protect On
   - Auto-Protect Off

Fine-tune Auto-Protect performance

In Mac OS X v10.1 Auto-Protect does not affect your computer's performance.

If you choose the highest level of automatic protection, you might notice that your computer's performance is affected during some activities.

You can adjust protection activity. Before making adjustments, try to determine the activity that seems to cause performance impairment, and make adjustments related to that activity.

If you notice a decrease in your computer's performance, lower the levels of protection for Auto-Protect.

To minimize protection levels in Norton AntiVirus

1. In the General Preferences dialog box, under Automatic protection level, select one of the following:
   - Minimal Protection
   - No Protection
2. Under Scanning level for compressed files, click **Do not scan compressed files**.

3 In the Custom Preferences dialog box, select the following:

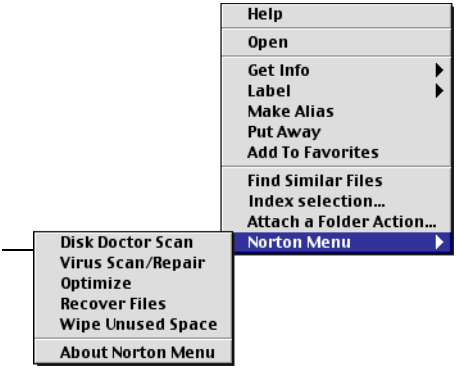
Prevention preferences	Turn off the setting that monitors virus-like activities.
Scan preferences	Turn off automatic scanning of files when opened and programs when launched.
Compression preferences	Limit the number of file types that are scanned.
SafeZones	Limit the number of SafeZones by clicking **Disable SafeZones**, or click **Custom** and limit the selected SafeZones protected by Auto-Protect.

For more information on Norton AntiVirus preferences, see “Customizing Norton AntiVirus for Macintosh” on page 87.

Perform scans using contextual menus

Contextual menus are not available in Norton AntiVirus for Mac OS X v10.1.

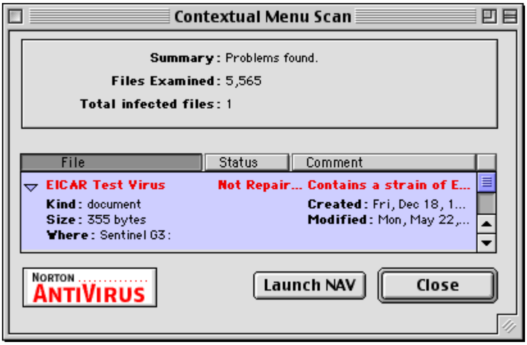
You can use the Macintosh OS contextual menu to scan a disk or item without starting Norton AntiVirus.



Contextual menu lets you scan for viruses without starting Norton AntiVirus

To perform scans using the contextual menu

1. Press **Control**, then select a disk, folder, or file icon.
2. On the contextual menu, click **Norton Menu > Virus Scan**.
   The Contextual Menu Scan scans the selected item.



Contextual Menu Scan

Summary: Problems found.
Files Examined: 5,565
Total infected files: 1

File	Status	Comment
EICAR Test Virus	Not Repair...	Contains a strain of E...
Kind: document **Size:** 355 bytes **Where:** Sentinel G3:		**Created:** Fri, Dec 18, 1... **Modified:** Mon, May 22,...

3. If you need to repair a virus, click **Launch NAV** to run Norton AntiVirus.

For more information

Norton AntiVirus provides Help, a Read Me file, and this User’s Guide in PDF format.

Access Help

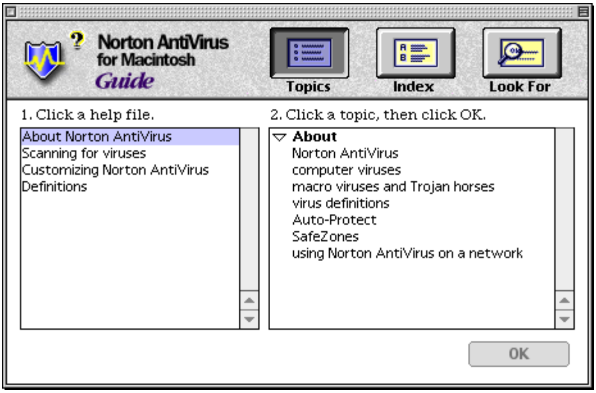
Norton AntiVirus has an extensive, interactive Apple Guide Help system that you can access from open dialog boxes or windows.

Norton AntiVirus for Mac OS X v10.1 has HTML Help files that you can read using the Apple Help Viewer.

To use Apple Guide Help in Mac OS 8.1–9.x

1 Do one of the following:

- In the upper right-hand corner of a dialog box or window, click **Help**.
- On the Help menu, click **Norton AntiVirus Help**.



1. Click a help file.

About Norton AntiVirus
Scanning for viruses
Customizing Norton AntiVirus
Definitions

2. Click a topic, then click OK.

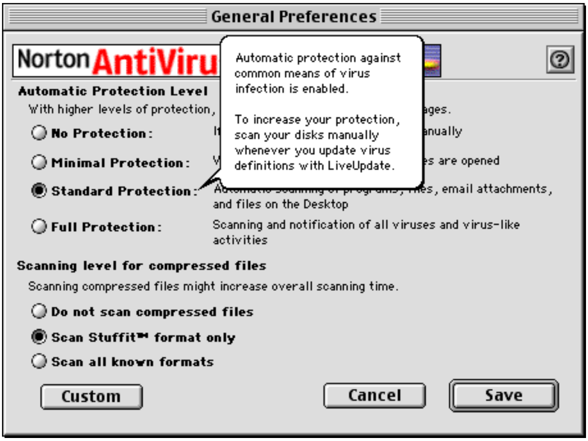
▽ **About**
Norton AntiVirus
computer viruses
macro viruses and Trojan horses
virus definitions
Auto-Protect
SafeZones
using Norton AntiVirus on a network

2 In the Norton AntiVirus for Macintosh Guide, do one of the following:

- Select a topic for more information.
- Follow the steps in the Guide window.

Use Balloon Help in Mac OS 8.1-9.x

You can use Balloon Help to familiarize yourself with the menu commands and dialog box options in Norton AntiVirus for Mac OS 8.1-9.x. With Balloon Help turned on, a descriptive text balloon appears when you move the cursor over a dialog box option, menu, or window item.



General Preferences

Norton AntiViru

Automatic Protection Level

With higher levels of protection, ges.

○ **No Protection:** I nually

○ **Minimal Protection:** W s are opened

● **Standard Protection:** A es, email attachments, and files on the Desktop

○ **Full Protection:** Scanning and notification of all viruses and virus-like activities

Scanning level for compressed files

Scanning compressed files might increase overall scanning time.

○ **Do not scan compressed files**

● **Scan Stuffit™ format only**

○ **Scan all known formats**

Automatic protection against common means of virus infection is enabled.

To increase your protection, scan your disks manually whenever you update virus definitions with LiveUpdate.

To turn on Balloon Help

- On the Help menu, click **Show Balloons**.
  A text balloon appears when you move the cursor over an item for which Balloon Help is available.

To turn off Balloon Help

- On the Help menu, click **Hide Balloons**.

Use the Apple Help Viewer in Mac OS X v10.1

Opening Help in Norton AntiVirus for Mac OS X v10.1 displays the Apple Help Viewer with a list of Help topics.

To use Help in Mac OS X v10.1

1. On the Help menu, click **Norton AntiVirus Help**.
2. On the list of Help topics, select a topic to read about it.

Open the Read Me file

The Read Me file on the Norton AntiVirus for Macintosh CD contains information that was unavailable at the time this User's Guide was published

To open the Read Me file

1. Insert the Norton AntiVirus for Macintosh CD into your CD-ROM drive.
2. Open the folder for the version of Norton AntiVirus that you have installed.
3. Double-click the **Read Me** file.

Access the User's Guide PDF

The *Norton AntiVirus for Macintosh User's Guide* is available in printable Adobe Acrobat PDF format on the CD. An Adobe Acrobat Reader can be installed if it is not already on your computer.

You cannot view the PDF if you start your computer from the CD, because Acrobat Reader does not run when you start from a locked device.

If you are using Mac OS X v10.1, you do not need to install the Adobe Acrobat Reader. You can use Preview in Mac OS X v10.1 to read the User's Guide PDF.

To install Adobe Acrobat Reader

1. In the Norton AntiVirus for Macintosh CD window, open the **Documentation** folder.
2. Double-click **Adobe Acrobat Reader installer**.
3. Follow the prompts to select a folder for Adobe Acrobat Reader and complete the installation.

To open the PDF

1. In the Norton AntiVirus for Macintosh CD window, open the **Documentation** folder.
2. Double-click **NAV User's Guide PDF**.

You can also drag the PDF to your hard disk. It needs approximately 1.2 MB of disk space.

Keeping current with LiveUpdate

4

LiveUpdate updates all Symantec products installed on your computer, as well as its own program files. If you have Norton AntiVirus installed, LiveUpdate also updates the files used by Norton AntiVirus to keep your virus protection current.

Using your existing Internet connection, LiveUpdate connects to the Symantec LiveUpdate server, checks for available updates, then downloads and installs them.

⚠ If you have installed Norton AntiVirus in Mac OS X v10.1 and Mac OS 9 and want to update features in both versions, you must run LiveUpdate separately in Mac OS X and Mac OS 9.

About program updates

Program updates are minor improvements to your installed product, usually available for download from a Web site. These differ from *product upgrades*, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called *patches*. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It locates and downloads files from an Internet site, then installs them, and deletes the leftover files from your computer.

About protection updates

One of the most common reasons for computer virus infections is that you have not updated your protection files regularly. Symantec provides online access to protection updates by subscription.

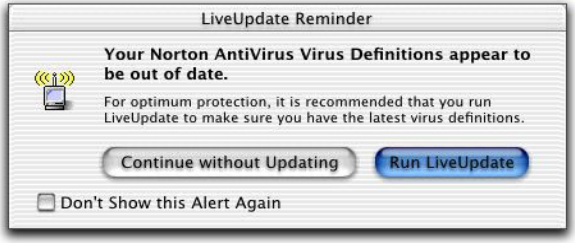
The virus definition service provides access to the latest virus signatures and other technology from Symantec. Norton AntiVirus, Norton SystemWorks, and Norton Internet Security use the updates available from the virus definition service to detect the newest virus threats.

See "Subscription policy" on page 136.

The initial subscription is included with the purchase of the product.

In Mac OS X, Norton AntiVirus has a setting to remind you to update your virus definitions if the current virus definitions are over one month (30 days) old, or are dated the previous year.

The following alert appears when it's time to update virus definitions:



LiveUpdate Reminder

Your Norton AntiVirus Virus Definitions appear to be out of date.

For optimum protection, it is recommended that you run LiveUpdate to make sure you have the latest virus definitions.

When you should update

See "Schedule future updates" on page 55.

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate at least once a month.

If you have Norton AntiVirus, Norton Personal Firewall, Norton Internet Security, or Norton SystemWorks installed, update at least once a month to ensure that you have the latest virus definitions and firewall protection.

Before updating

In some cases there are preparations you must make before running LiveUpdate. For example, if you use America Online (AOL) as your Internet Service Provider (ISP), you must log on to AOL before you use LiveUpdate.

If you use America Online to connect

If you use America Online (AOL) as your Internet Service Provider (ISP), you need to log on to AOL before you use LiveUpdate.

To use LiveUpdate with AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Start LiveUpdate.
4. Follow the instructions in "Update procedures" on page 52.
5. When the LiveUpdate session is complete, close your AOL browser. If your LiveUpdate session requires that you restart your computer, disconnect from AOL before restarting.

If you update on an internal network

If you run LiveUpdate on a Macintosh that is connected to a network that is within a company firewall, your network administrator might set up an internal LiveUpdate server on your network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can download new update files from the Symantec Web site.

To download virus definitions from the Symantec Web site

1. Start your Internet browser and go to the following site:
   http://securityresponse.symantec.com/avcenter/defs.download.html
   If this page doesn't load, go to http://securityresponse.symantec.com and click the **Download Virus Definitions** link, then click the **Download Virus Definitions Updates** link.
2. On the Download Virus Definitions page, click **Norton AntiVirus for Macintosh**.

3 Click **Download Updates**.

4 On the Download Updates page, select the file to download.
Be sure to select files for the appropriate version of your product.
Information about the update is included with the download.

To download product updates from the Symantec Web site

1 Start your Internet browser and go to the following site:
http://securityresponse.symantec.com/downloads/
If this page doesn’t load, go to http://securityresponse.symantec.com and click **downloads**.

2 On the downloads page, in the product updates list, select the product for which you want an update.

3 Click **Browse**.

4 On the product page, select the version of the product.

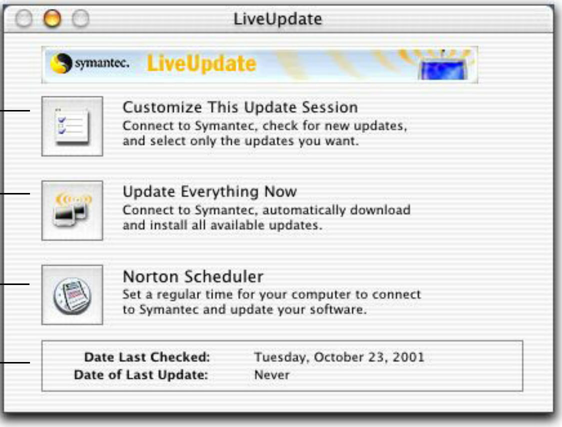
5 Click **Continue**.

6 On the updates page, select the file to download.
Information about the update is included with the download.

Update procedures

See “Schedule future updates” on page 55.

You can have LiveUpdate look for all updates at once, or select individual items to update. You can also schedule a future LiveUpdate session.



Customize This Update Session
Connect to Symantec, check for new updates, and select only the updates you want.

Update Everything Now
Connect to Symantec, automatically download and install all available updates.

Norton Scheduler
Set a regular time for your computer to connect to Symantec and update your software.

Date Last Checked: Tuesday, October 23, 2001
Date of Last Update: Never

Select items to update during this session

Updates all installed components

Lets you schedule specific updates

Indicates the last update activity

Update everything now

Updating all available files is the fastest method to ensure the latest protection for all your Symantec products.

To update everything now

1. On the Utilities menu, click **LiveUpdate**.
2. Click **Update Everything Now**.
   A status dialog box keeps you informed of the file transfer process.
3. If you want to skip a file download, click **Skip File**.
   The file transfer takes a few minutes. When it is complete, LiveUpdate notifies you. See "View the LiveUpdate Summary" on page 54.

Customize a LiveUpdate session

If you want to update only one or two items, you can select them and omit items that you don't want to update.

To customize a LiveUpdate session

1. In the LiveUpdate window, click **Customize This Update Session**.
   LiveUpdate presents a list of available updates. By default, all are checked for inclusion in this update session. If your files are already up-to-date, no items are available for selection.
2. Uncheck the items that you don't want to update.
3. Click **Update**.
   The file transfer takes a few minutes. When it is complete, LiveUpdate notifies you. See "View the LiveUpdate Summary" on page 54.

After updating

When a LiveUpdate session is complete, the LiveUpdate Summary window displays a list of what was updated, along with brief notes.

After updating Norton AntiVirus, LiveUpdate also downloads a What's New file, which is placed on the desktop.

View the LiveUpdate Summary

The LiveUpdate Summary dialog box displays a summary of the activity and a list of products updated in this session.

Some updates require that you restart your computer. When this recommendation appears in the summary description, the Restart button is available.

To restart after a LiveUpdate session

❖ In the LiveUpdate Summary window, click **Restart**.

Read the LiveUpdate What's New file

LiveUpdate places a What's New file on the desktop. This contains details of what files were updated by LiveUpdate.

To do this	Follow these steps
Read the What's New file.	Double-click the file.
Close the What's New file.	Press **Command-Q.**
Delete the What's New file.	Drag it to the Trash.

Empty the Trash after a LiveUpdate session

After you update program files, LiveUpdate moves the older, discarded files to the Trash. If you haven't already restarted after updating, you might get a message that these files are in use. After you restart your computer, you can empty the Trash.

Check product version numbers and dates

The LiveUpdate window displays the version numbers and dates of the most recent updates.

You can also check the version numbers and dates in the product's About box, accessible from the product menu in Mac OS X v10.1, or the Apple menu in Mac OS 8.1–9.x.

To view an application's About box

1. Start your product.
2. Do one of the following:
   - In Mac OS X v10.1, on the product menu, click **About <product name>**.
   - In Mac OS 8.1–9.x, on the Apple menu, click **About <product name>**.
     The About box lists version number and copyright dates.
3. When you've finished viewing the About box, click **OK**.

Schedule future updates

⚠ You can schedule an update in both Mac OS X v10.1 and in Mac OS 9. The operating system in which the update is scheduled must be running for the scheduled event to occur. In addition, in Mac OS X v10.1, the user who scheduled the event must be logged on. If these conditions are not true, the event occurs the next time the operating system is started, with the correct user logged on, if applicable.

You can set up events to run at a scheduled time, without your participation.

If your Macintosh is turned off during the time an event should take place, the event occurs the next time that you start your Macintosh.

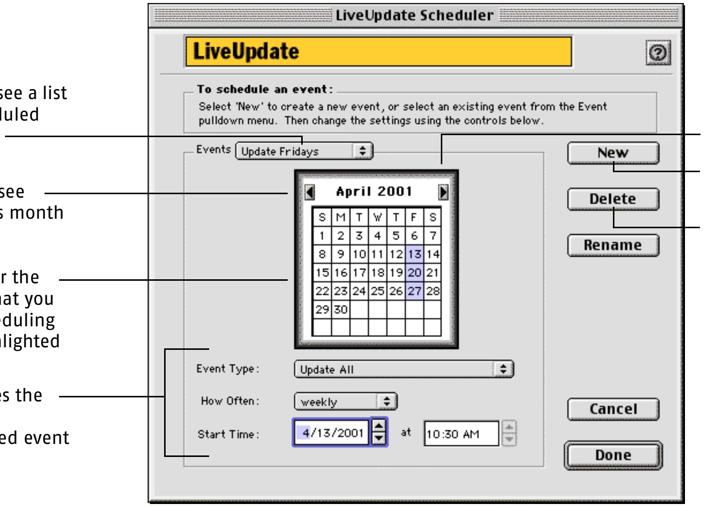
Before scheduling an update, test it once manually. See "Update everything now" on page 53, and "Customize a LiveUpdate session" on page 53.

Schedule future updates in Mac OS 8.1–9.x

You can add, edit, and delete scheduled events in Mac OS 8.1–9.x.

To schedule future updates in Mac OS 8.1–9.x

1 In the LiveUpdate main window, click **Schedule Future Updates**.



To schedule an event:

Select 'New' to create a new event, or select an existing event from the Event pulldown menu. Then change the settings using the controls below.

Events: Update Fridays

Event Type: Update All

How Often: weekly

Start Time: 4/13/2001 at 10:30 AM

Click to see a list of scheduled events

Click to see previous month

Dates for the event that you are scheduling are highlighted

Describes the selected scheduled event

Click to see next month

Create a new scheduled event

Delete a scheduled event

2 Click **New**.

3 In the Scheduled Event name text box, type a descriptive name, for example, Update Fridays.

4 Click **OK**.

5 In the Event Type list, specify the item to update.
Your choices are:

Update All	Updates all installed products.
Update <Product Name>	Updates the product that you select. The names of installed Symantec products appear in the list.

6 In the How Often list, specify when the update should occur.
Your choices are:

once	Runs the event one time only on the indicated day and time
daily	Runs the event daily at the indicated time
weekdays	Runs the event every weekday, Mondays through Fridays, at the indicated time
weekly	Updates once a week on the specified day and at the specified time
monthly	Runs the event monthly at the indicated time
disabled	Never runs the event

The days on which the updates occur appear highlighted in the calendar.

7 Finish scheduling the update by typing the time and date:

- Click the **Hour** text box and use the arrow keys to set the start hour.
- Click the **Minute** text box to set the start minute.

8 Click **Done**.

To edit a scheduled event

1 In the LiveUpdate main window, click **Schedule Future Updates**.

2 In the Events list, click the scheduled event that you want to change.

3 Make your changes.
For a description of the scheduling options, see "Schedule future updates in Mac OS 8.1–9.x" on page 55.

4 To change the event name, click **Rename** and type a new name.

5 Click **Done**.

To delete a scheduled event

1 In the LiveUpdate main window, click **Schedule Future Updates**.

2 In the Events list, select the scheduled event to delete.

3 Click **Delete**.

4 Click **Yes** to verify deletion.

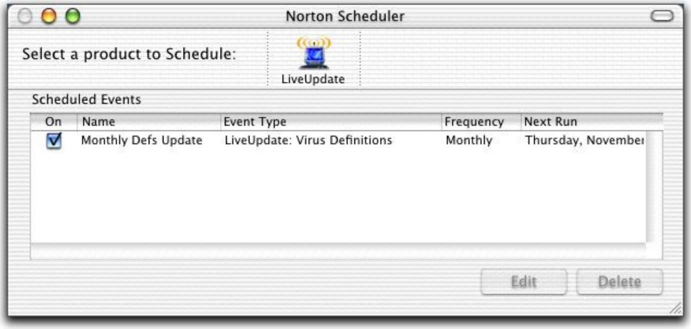
5 Click **Done**.

Schedule future updates in Mac OS X v10.1

You can add, edit, delete, and disable scheduled events in Mac OS X. You can also reset all scheduled events to the default events and settings.

To schedule future updates in Mac OS X

1 In the LiveUpdate main window, click **Norton Scheduler**.

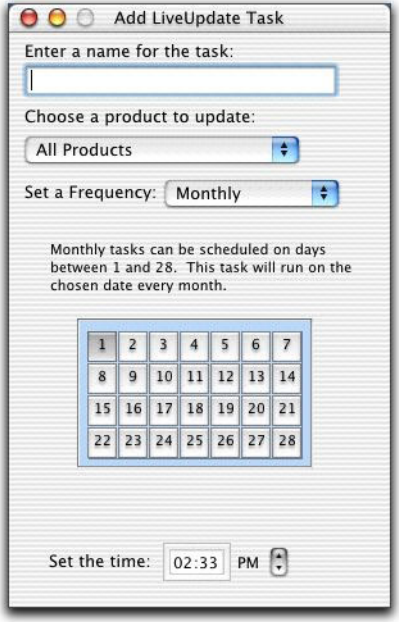


Select a product to Schedule:

Scheduled Events

On	Name	Event Type	Frequency	Next Run
☑	Monthly Defs Update	LiveUpdate: Virus Definitions	Monthly	Thursday, Novembe

2 Click **LiveUpdate**.



Enter a name for the task:

Choose a product to update: All Products

Set a Frequency: Monthly

Monthly tasks can be scheduled on days between 1 and 28. This task will run on the chosen date every month.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Set the time: 02:33 PM

3 Type a descriptive name for the LiveUpdate task, for example, Update Fridays.

4 In the Choose a product to update list, specify the item to update.
Your choices are:

All Products	Updates all installed products.
<Product Name>	Updates the product that you select. The names of installed Symantec products appear in the list.

5 In the Set a Frequency list, specify when the update should occur.
Your choices are:

Monthly	Runs the event monthly on the indicated date and time. You can choose a date from the first of the month to the twenty-eighth.
Weekly	Updates once a week on the specified day and at the specified time.
Daily	Runs the event daily at the indicated time.
Annually	Runs the event each year on the indicated day and time. You can schedule the event up to one year in advance.

6 Close the **Add LiveUpdate Task** window.

7 In the Save LiveUpdate Task dialog box, click **Save**.

Edit scheduled events

You can make changes to the events that you schedule.

To edit a scheduled event

1 In the LiveUpdate main window, click **Norton Scheduler**.

2 In the Scheduled Events list, select the scheduled event that you want to change.

3 Click **Edit**.

4 Make your changes.
For a description of the scheduling options, see “Schedule future updates in Mac OS X v10.1” on page 58.

5 To change the event name, type a new name in the name field.

6. Close the **Add LiveUpdate Task** window.
7. In the Save LiveUpdate Task dialog box, click **Save**.

Delete scheduled events

You can delete events that you no longer want.

To delete a scheduled event

1. In the LiveUpdate main window, click **Norton Scheduler**.
2. In the Scheduled Events list, select the scheduled event that you want to delete.
3. Click **Delete**.
4. In the verification box that appears, click **Delete** to verify that you want to delete the event.

Disable scheduled events

You can disable scheduled events without deleting them in case you want to enable them later.

To disable a scheduled event

1. In the LiveUpdate main window, click **Norton Scheduler**.
2. In the Scheduled Events list, uncheck the event that you want to disable.
3. To enable the event, check it again.

Reset scheduled tasks

If you want to delete all scheduled tasks that you have added and reset the scheduled tasks to the original default tasks, use Reset Scheduled Tasks.

The default tasks that are set depend on which Symantec products you have installed. All default tasks can be edited to change their schedule.

Product	Default task
Norton Personal Firewall	None.
Norton AntiVirus	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month.
Norton Internet Security	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month.

Product	Default task
Norton Utilities	Daily FileSaver scan to update your disk directory information. Set to run at noon.
Norton SystemWorks	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month. Daily FileSaver scan to update your disk directory information. Set to run at noon.

To reset scheduled tasks

1. In the LiveUpdate main window, click **Norton Scheduler**.
2. On the Norton Scheduler menu, click **Reset Scheduled Tasks**.
3. In the verification window, click **Reset**.

Protecting disks, files, and data from viruses

5

Viruses activate when you launch an infected program, start your computer from a disk that has infected system files, access a floppy disk or other *removable media* (disks that can be removed, such as floppy disks, disk cartridges, CDs, and Zip disks) that has infected desktop files, or access a document containing a macro virus.

Although Norton AntiVirus Auto-Protect monitors your computer for viruses by scanning files when they are opened or moved, scan all disks or removable media before you use them, as Auto-Protect might not catch viruses that have infected files that haven't been opened, moved to a SafeZone, or scanned. With Norton AntiVirus you can scan any file, folder, or disk for viruses.

Scan disks, folders, and files

See "Perform scans using contextual menus" on page 43.

You can start the Norton AntiVirus main program or, in Norton AntiVirus for Mac OS 8.1-9.x, use the contextual menu, to scan your disks.

In Mac OS X v10.1, Norton AntiVirus can scan only those files to which you have access permission. Even if you are logged on as an administrator, there are certain system files and directories that cannot be scanned. Those files can be scanned only if you are logged on with root access. However, unless you log on as root when you work on your computer, there is almost no chance that those files could be infected, as Mac OS X v10.1 is set by default to have the root account disabled.

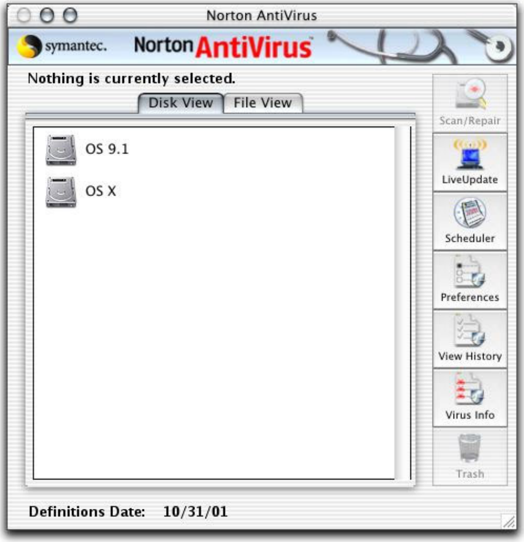
If you never log on as root, performing scans while logged on as an administrator catches any viruses the computer might have acquired. If you log on as root, perform scans under the same logon. You can also restart from the CD and scan using Norton AntiVirus for Mac OS 8.1-9.x to avoid access problems and permissions errors.

See "About Compression Preferences" on page 105.

You can customize the way Norton AntiVirus performs scans. Norton AntiVirus can check compressed files for viruses, but not encrypted files. Encrypted files, which normally require a password to open them, must be decrypted before you scan them.

To scan disks, folders, and files for viruses

1 Start Norton AntiVirus.



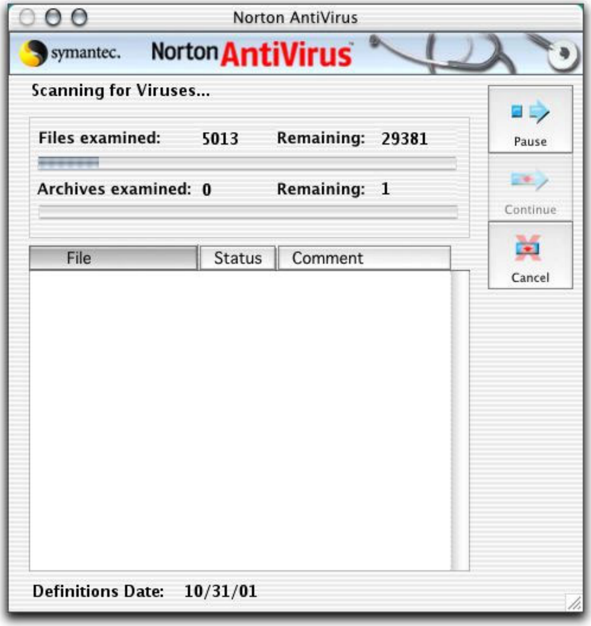
Nothing is currently selected.

Definitions Date: 10/31/01

2 In the Norton AntiVirus main window, select the disks to scan:

- View the contents of the disk by clicking the triangle next to the disk name.
- On the File View tab, select folders or files.

3 Click **Scan** or **Scan/Repair**.
In Mac OS 8-9.x if the Virus Scanning Preferences are not set to repair infected files automatically, the button name is Scan. When the scan is complete, the results are shown in the window. The top pane of the window shows a summary of the scan. The bottom pane of the window lists any files that were found to have problems.



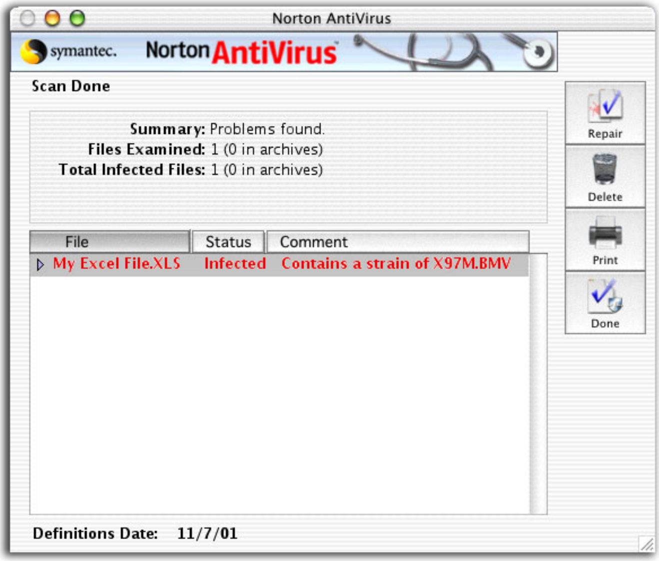
Scanning for Viruses...

Files examined: 5013 Remaining: 29381

Archives examined: 0 Remaining: 1

Definitions Date: 10/31/01

4 To view details of a selected file, click the triangle beside the file.



Scan Done

Summary: Problems found.
Files Examined: 1 (0 in archives)
Total Infected Files: 1 (0 in archives)

File	Status	Comment
▷ My Excel File.XLS	Infected	Contains a strain of X97M.BMV

Definitions Date: 11/7/01

If problems are found during a scan

Norton AntiVirus is designed to help keep your computer virus-free. In most cases, an infected file can be repaired automatically. In some cases, you may need to take further action.

In Mac OS 8.1-9.x, if a virus is found and Auto-Repair is enabled, the file is automatically repaired. In Mac OS X v10.1, the file is automatically repaired if you have Automatic Repair On checked on the General tab of the Preferences window.

See "If Norton AntiVirus can't repair a file" on page 81.

If the virus is not repaired, the file can be removed. Removing a file prevents it from reinfecting your computer or damaging other files.

Scan email attachments

Norton AntiVirus provides automatic scanning of email messages. Because Norton AntiVirus for Mac OS X v10.1 scans all files closed with write permission, email attachments are files scanned.

See "Access Custom Preferences in Mac OS 8.1-9.x" on page 90.

If you are using Norton AntiVirus for Mac OS 8.1-9.x, email attachments are automatically scanned if you have checked that option in Preferences. In addition, if your email program is one that Norton AntiVirus supports, Auto-Protect automatically scans all email attachments when they are downloaded.

To determine if your email program is supported

1. In your Internet browser, navigate to the Symantec Service and Support Web site at: www.symantec.com/techsupp/
2. On the Service and Support Web page, click **I am a home / small business user**.
3. On the home computing and small business page, select **Norton AntiVirus for Macintosh** as the product, **8.x** as the version, then click **continue**.
4. On the stage one page, select **solving a software issue** as what you need help with, **to solve some other software issue** as what you want, and click **continue**.
5. On the stage two page, click **continue to knowledge base**.
6. In the search field, type **email clients**.
7. Click **search**.
8. On the stage three page under search results, click **Which email clients does NAV for Macintosh 8.0 support for email scanning?**

Decontamination procedures

If you think that a virus has infected your computer and you are afraid that there might be a virus in memory, use the Norton AntiVirus for Macintosh CD to restart your computer and remove the virus. For detailed instructions see "Start from the CD" on page 21 and "Scan for viruses" on page 22.

View and print scan history

Norton AntiVirus automatically saves a report of each scan. You can view and print these scan results at the end of a scan. You can also review previous scans in the History file.

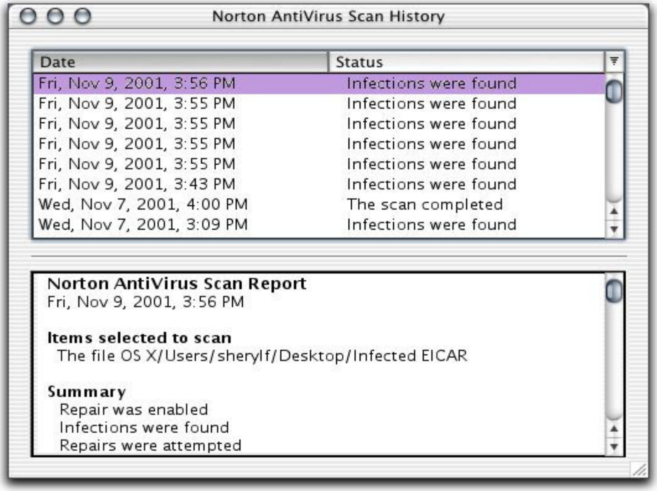
Save and print scan reports

See "About Report Preferences" on page 103.

At the end of a scan, you can save the scan results in a data file. You can specify the data file format in Preferences. Saving a scan report in a specific file format relates it to a word processing program. You can print a scan report from the Scan Results window or from the Scan History window.

To select a scan report to save or print

1 In the Norton AntiVirus main window, click **View History**.



Date	Status
Fri, Nov 9, 2001, 3:56 PM	Infections were found
Fri, Nov 9, 2001, 3:55 PM	Infections were found
Fri, Nov 9, 2001, 3:55 PM	Infections were found
Fri, Nov 9, 2001, 3:55 PM	Infections were found
Fri, Nov 9, 2001, 3:55 PM	Infections were found
Fri, Nov 9, 2001, 3:43 PM	Infections were found
Wed, Nov 7, 2001, 4:00 PM	The scan completed
Wed, Nov 7, 2001, 3:09 PM	Infections were found

Norton AntiVirus Scan Report
Fri, Nov 9, 2001, 3:56 PM

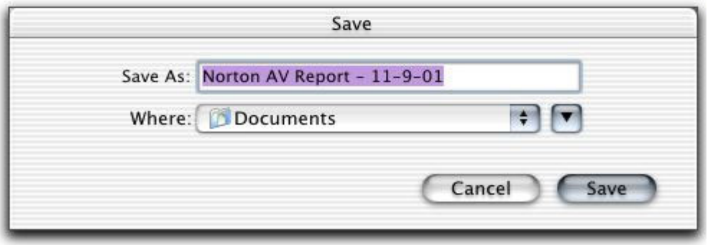
Items selected to scan
The file OS X/Users/sherylf/Desktop/Infected EICAR

Summary
Repair was enabled
Infections were found
Repairs were attempted

2 In the Norton AntiVirus Scan History window, in the top pane, select the report to view.
The details appear in the lower pane of the window.

To save the selected scan report

1 On the File menu, click **Save Report As**.



Save

Save As: Norton AV Report - 11-9-01

Where: Documents

2 In the dialog box that appears, specify a name and location for the file. The default file name is <Untitled> Scan Report.

3 In the Save dialog box, click **Save**.

To print the selected scan report

1 Do one of the following:

- If you are still viewing the scan results, click **Print**.
- If you have selected the report in the Scan History window, on the File menu, click **Print Report**.

2 In the Print dialog box, select the printing options for the report.

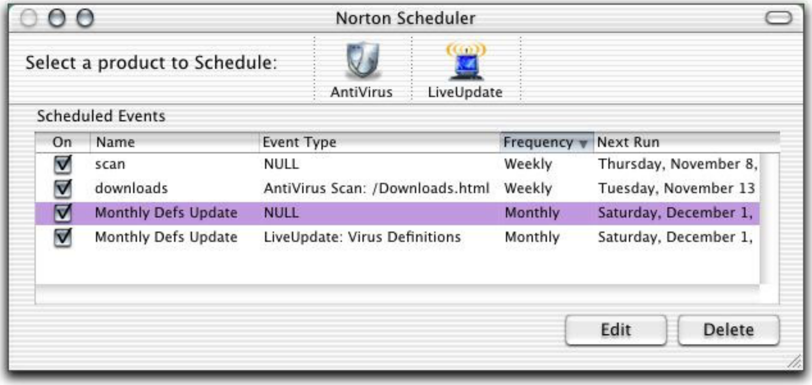
3 Click **Print**.

Add scheduled Norton AntiVirus scans

You can add scheduled scans of all or a part of your computer for your convenience. The scan results of a spontaneous or scheduled scan are displayed as scan results in the main Norton AntiVirus window.

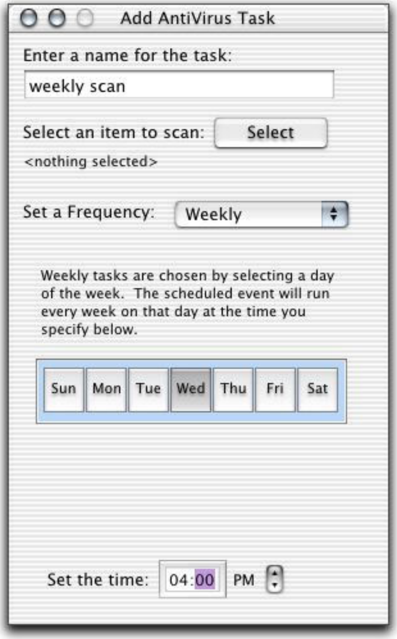
To add scheduled Norton AntiVirus scans

1 In the Norton Scheduler window, click **AntiVirus**.



On	Name	Event Type	Frequency	Next Run
☑	scan	NULL	Weekly	Thursday, November 8,
☑	downloads	AntiVirus Scan: /Downloads.html	Weekly	Tuesday, November 13
☑	Monthly Defs Update	NULL	Monthly	Saturday, December 1,
☑	Monthly Defs Update	LiveUpdate: Virus Definitions	Monthly	Saturday, December 1,

2 Type a descriptive name for the task, for example, weekly scan.



Enter a name for the task: weekly scan

Select an item to scan: <nothing selected>

Set a Frequency: Weekly

Weekly tasks are chosen by selecting a day of the week. The scheduled event will run every week on that day at the time you specify below.

Set the time: 04:00 PM

3 To select an item to scan, click **Select**.

4 In the Select a scan target window, select the portion of your computer that you want to scan.

5 Click **Open**.

6 In the Set a Frequency list, specify when the scan should occur. Your choices are:

Monthly	Runs the event monthly at the indicated date and time. You can select a date from the first of the month to the twenty-eighth.
Weekly	Updates once a week on the specified day and at the specified time.
Weekly	Runs the event daily at the indicated time.
Annually	Runs the event each year on the indicated day, and at the indicated time. You can schedule the event up to one year in advance.

7 Close the Add AntiVirus Task window.

8 In the Save AntiVirus Task dialog box, click **Save**.

To make virus prevention as easy as possible, schedule these activities:

More information	**Activity**
See "Add scheduled Norton AntiVirus scans" on page 69.	Virus scans to occur at specified times
See "Schedule future updates" on page 55.	Automatic updates of virus definitions with LiveUpdate

If your Macintosh is turned off during the time an event should take place, the event occurs the next time you start your Macintosh.

Edit scheduled events

You can make changes to the events that you schedule.

To edit a scheduled event

1. In the Scheduled Events list, select the scheduled event that you want to change.
2. Click **Edit**.
3. Make your changes.
4. To change the event name, in the name field, type a new name.
5. Close the Edit Task window.
6. In the Save Task dialog box, click **Save**.

Delete scheduled events

You can delete scheduled events that you no longer want.

To delete a scheduled event

1. In the Scheduled Events list, select the scheduled event that you want to delete.
2. Click **Delete**.
3. In the verification box that appears, click **Delete** to verify that you want to delete the event.

Disable scheduled events

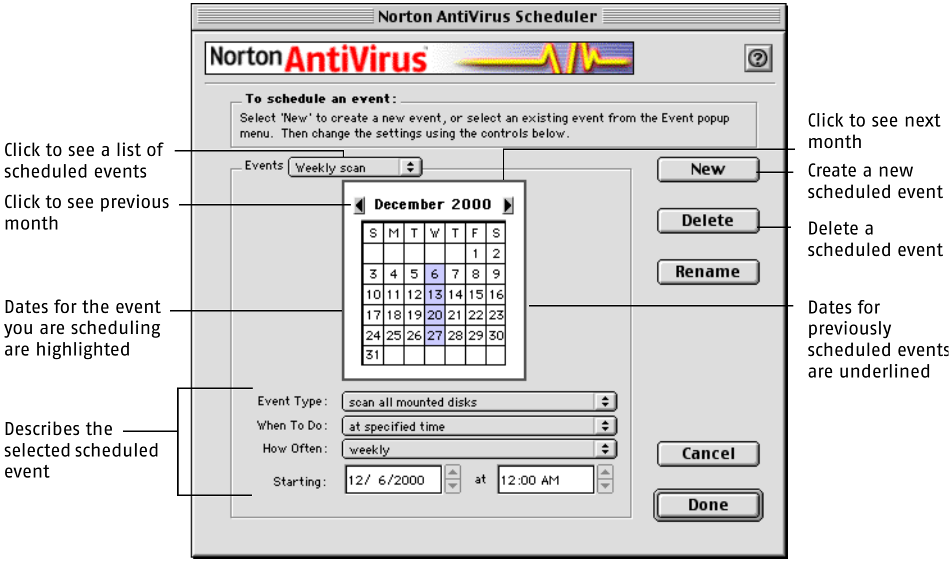
You can disable scheduled events without deleting them in case you want to enable them later.

To disable a scheduled event

1. In the Scheduled Events list, uncheck the event that you want to disable.
2. To enable the event, check it again.

To schedule a scan in Mac OS 8.1-9.x

1 On the Tools menu, click **Scheduler**.



Norton AntiVirus Scheduler

To schedule an event:

Select 'New' to create a new event, or select an existing event from the Event popup menu. Then change the settings using the controls below.

Events: Weekly scan

December 2000

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Event Type: scan all mounted disks

When To Do: at specified time

How Often: weekly

Starting: 12/ 6/2000 at 12:00 AM

Click to see a list of scheduled events

Click to see previous month

Dates for the event you are scheduling are highlighted

Describes the selected scheduled event

Click to see next month

Create a new scheduled event

Delete a scheduled event

Dates for previously scheduled events are underlined

2 Click **New**.

3 In the dialog box that appears, type the event name in the text field.

4 Click **OK**.

5 In the Event Type list, specify the item to scan. Your choices are:

Scan System Folder	Scans the System folder on the startup disk
Scan System Disk	Scans the entire startup disk
Scan All Local Disks	Scans all disks physically connected to your computer
Scan All Network Disks	Scans all network drives mounted at the time the scan runs
Scan All Mounted Disks	Scans all local and network drives mounted at the time the scan runs

6 In the When To Do list, specify when the scan should occur. Your choices are:

At Specified Time	Lets you decide the time for the scan to occur
At Startup	Scans for viruses each time your computer starts up
At Shutdown	Scans for viruses each time your computer shuts down

7 In the How Often list, specify the frequency of the scan. Your choices are:

Disabled	Saves all settings for the event, but never runs it
Once	Runs the event one time only at the indicated time
Hourly	Runs the event hourly at the indicated time
Daily	Runs the event daily on the indicated day
Weekdays	Runs the event every weekday, Mondays through Fridays, at the indicated time
Monthly	Runs the event monthly at the indicated time
Always	Always runs the event

8 Finish scheduling the scan by typing the correct time and date information.
This option is not available if the scan occurs at startup or shutdown.

9 Click **Done**.

Perform a scan from the command line

Use the Command Line Scanner to run scans from the command line and to obtain scan reports and save them in your specified destination. Create scripts to be incorporated into other UNIX maintenance scripts.

Following are a few examples of how you can customize the features of Command Line Scanner to run the scans that you want.

- navx/
  To scan your system drive with default options
- navx -a -r /Users/steve/
  To scan, without repairing, the files in the home folder of user steve, and report the status of all files
- navx -ar /Users/steve/
  To scan, without repairing, the files in the home folder of user steve, and report the status of all files
- navx -o ~/myReportFile /tmp
  To scan the files in /tmp, and store the report in your home folder
- navx -a -o ~/myReportFile /tmp > scansummary.log
  To scan the files in /tmp, store the complete report in your home folder, and the summary in a log

To scan a file using the Command Line Scanner

1. Open Terminal.
2. At the prompt, type **navx**.
3. Type the command you want. Your options are:

-a	Reports all files scanned regardless of damage or threat.
-f	Forces the scan to run even if the output file specified with -o cannot be created or opened.
-h	Reports on files that were inaccessible for scanning.
-q	Quiet, only the summary text is displayed on the screen.
-r	Does not repair files with defined threats.
-o <output filename>	Output appends to the file <output filename>. If -q is also selected, only the summary appears on the screen, but the full report is appended to <output filename>.

4. Enter the file you want to scan.
5. Press **Enter**.

What to do if a virus is found

6

If Norton AntiVirus reports a problem, find the section that best describes the problem, and then follow the instructions provided.

The message may not be discussed in this chapter. For more information about other messages, see "Mac OS 8.1-9.x and Mac OS X v10.1 messages" on page 121.

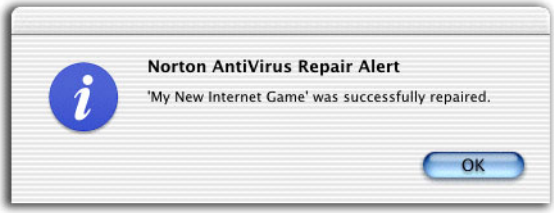
If Auto-Protect finds a virus

When a virus is found while Norton AntiVirus Auto-Protect is running, an alert displays what happened and what your options are.

Auto-Protect alerts you to any virus activity, whether the file is repaired automatically or not. Read the message carefully to determine whether you need to do anything.

If Auto-Protect finds a virus and repairs the file

When Norton AntiVirus Auto-Protect reports that it repaired an infected file, you don't have to do anything.



Norton AntiVirus Repair Alert

'My New Internet Game' was successfully repaired.

Even when Auto-Protect has repaired the infected file, ensure that no other viruses exist on your computer by scanning with Norton AntiVirus.

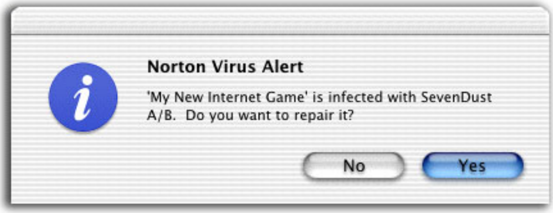
If Auto-Protect finds a virus but does not repair the file

See "About Scan Preferences" on page 95.

If you have set the Auto-Repair Scan preference to off, Auto-Protect informs you of infected files, but does not repair them.

To handle an infected file that has been detected but not repaired

1 Read the entire message.



Norton Virus Alert

'My New Internet Game' is infected with SevenDust A/B. Do you want to repair it?

2 Look for words that identify the type of problem.

3 Select the button of the action that you want to take.
Repairing is always the best choice. It eliminates the virus and restores the infected item automatically.

If Auto-Protect finds a virus and cannot repair the file

Auto-Protect may not be able to repair an infected file, whether or not you have requested Auto-Repair.

To delete an infected file that has been detected but cannot be repaired

1 Click **Yes** to run Norton AntiVirus and scan the file or folder containing the virus. See "Scan disks, folders, and files" on page 63.

2 In the scan window, you can view more details about the infected file. See "If Norton AntiVirus can't repair a file" on page 81.

3 In Mac OS 8.1-9.x, take further action as indicated in the scan window.

If removable media is infected

In Mac OS 8.1-9.x, when Standard Protection is set, Auto-Protect ejects infected removable media. Bypass this setting by holding down the Shift key while inserting the media.

To repair the infected media, use Norton AntiVirus to scan and repair it.

To repair infected removable media

1. Start Norton AntiVirus.
2. Insert the media while pressing **Shift** on your keyboard.
3. In the Norton AntiVirus main window, select the media to scan.
4. Click **Scan** or **Scan/Repair**.

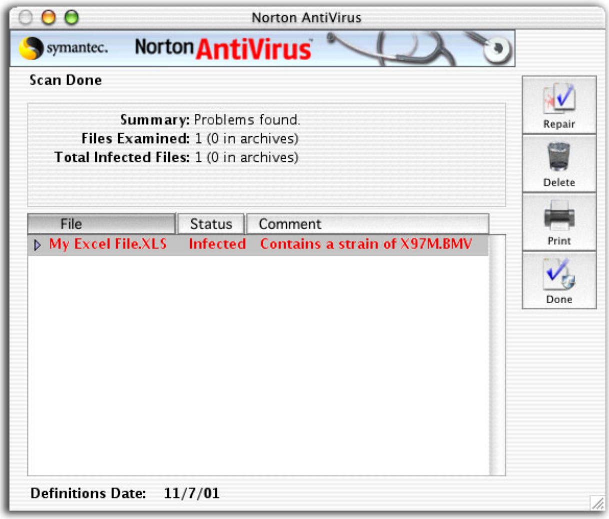
If a virus is found while scanning

If you are scanning with Norton AntiVirus and a virus is found, a Problem found alert appears in the scan window. Usually, infected files are repaired automatically and you don’t have to do anything else. To determine if the file was repaired or if you need to take further action, check the status of the file in the scan window.

To check the status of infected files in the scan window

1 In the Scan Results window, select the infected file.

2 Click the triangle to the left of the file to view more information about the file.



Scan Done

Summary: Problems found.
Files Examined: 1 (0 in archives)
Total Infected Files: 1 (0 in archives)

File	Status	Comment
▷ My Excel File.XLS	Infected	Contains a strain of X97M.BMV

Definitions Date: 11/7/01

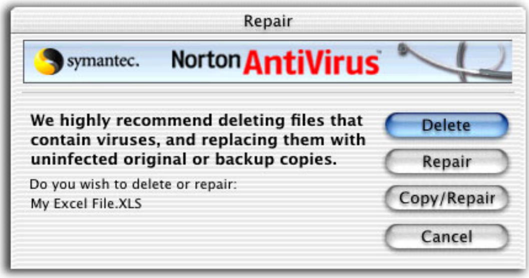
Repair infected files

If an infected file in the scan window was not repaired because Auto-Repair was turned off in Preferences, initiate the repair yourself.

To repair infected files

1 In the scan results list, select the files to repair.

2 Click **Repair**.



We highly recommend deleting files that contain viruses, and replacing them with uninfected original or backup copies.

Do you wish to delete or repair:
My Excel File.XLS

3 In the Repair dialog box, do one of the following:
   - Click **Repair**.
   - Click **Copy/Repair** if you want to create a backup copy of the file before it is repaired.

4 After repairing all infected files, scan your disks again to verify that there are no other infected files.

5 Check the repaired files to make sure that they function properly.
   For example, if you repaired a word processing program, start it, edit a file, save a file, and so on to make sure that it has been repaired correctly.

If you chose to have Norton AntiVirus make a backup copy of the infected file before you repaired it, delete the backup file once you are certain the repair worked correctly. The infected backup copy of the file is stored in the same directory as the original file. (The backup copy is named infected <file name> where <file name> is the name of the original file.)

If Norton AntiVirus can’t repair a file

See “Check product version numbers and dates” on page 54.

If Norton AntiVirus cannot repair the infected file, first make sure you have scanned with the latest virus definitions. If you are not sure that you have the latest definitions, use LiveUpdate. Then scan your hard disk with the latest virus definitions.

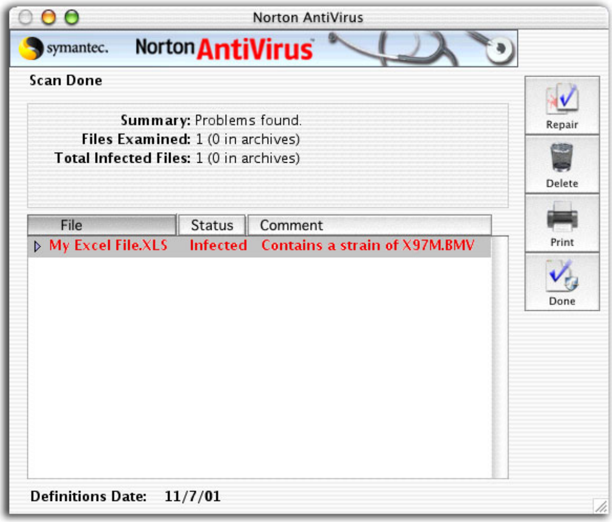
Delete infected files

Sometimes viruses damage a file beyond repair. If Norton AntiVirus finds an irreparable file, delete the infected file and replace it with an uninfected backup copy.

You can’t delete an infected file from an Auto-Protect alert. Delete it from the Norton AntiVirus scan window.

To delete an infected file

1 When prompted by the Auto-Protect alert to scan with Norton AntiVirus, click **Yes**.
Norton AntiVirus opens and scans the infected file. The Norton AntiVirus scan results window displays the infected file.



Scan Done

Summary: Problems found.
Files Examined: 1 (0 in archives)
Total Infected Files: 1 (0 in archives)

File	Status	Comment
My Excel File.XLS	Infected	Contains a strain of X97M.BMV

Definitions Date: 11/7/01

2 Select the infected file.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.
The Status column in the scan window shows that the file has been deleted.

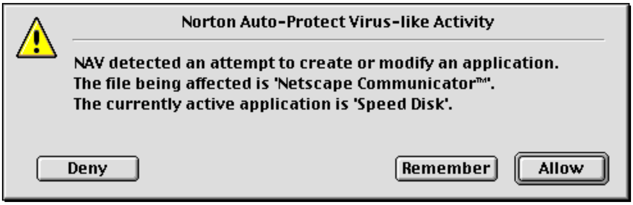
If you receive a Virus-like Activity alert in Mac OS 8.1-9.x

Virus-like Activity alerts are not generated in Norton AntiVirus for Mac OS X.

See "About Prevention Preferences" on page 98.

A virus-like activity is an activity that viruses often perform when spreading or damaging your files. A Virus-like Activity alert does not necessarily mean a virus is present. You can decide whether the operation is valid, for example, when you are installing software or decompressing a compressed archive.

When a virus-like activity is detected, an alert appears.


Norton Auto-Protect Virus-like Activity

NAV detected an attempt to create or modify an application.
The file being affected is 'Netscape Communicator™'.
The currently active application is 'Speed Disk'.

See "Keeping current with LiveUpdate" on page 49.

Make sure that you have the most recent virus definitions file. If the application contains an unknown virus, the newest virus definitions file may have a definition for it.

To respond to a Virus-like Activity alert

❖ Select one of the following:

Allow	Allow the activity if the message describes a valid activity for the application you are running, for example, if you are changing a system setting. This action is the default selection.
Deny	Deny the activity if it isn't related to what you are trying to do. If the Deny button is unavailable, the virus-like activity has proceeded too far for Norton AntiVirus to stop without causing damage or crashing the system. If this happens, note the file involved and the currently active application before continuing, then scan both files to check for known viruses.
Remember	Remember the activity if you don't want the alert to appear again. If the activity is valid for the application you are running and you don't want Norton AntiVirus to alert you when the same application performs the same activity in the future, click Remember. This activity is added to the Exceptions List. Future attempts to perform the same action by the same application will not trigger the activity alert. See "Manage virus-like activities" on page 109.

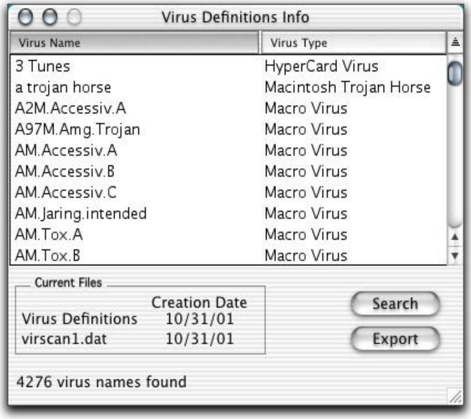
Look up virus names and definitions

You can look up a virus name from within the Norton AntiVirus application. The Virus Definitions Info dialog box lists the viruses in the current virus definitions file. To make sure you have the latest virus definitions, run LiveUpdate. You can export the list to a text file. You can also search the list for a specific virus.

To look up virus names

❖ Do one of the following:

- In Norton AntiVirus for Mac OS 8.1-9.x: On the Tools menu, click **Virus Definitions Info**.
- In Norton AntiVirus for Mac OS X v10.1: On the Window menu, click **Virus Info**.



Virus Name	Virus Type
3 Tunes	HyperCard Virus
a trojan horse	Macintosh Trojan Horse
A2M.Accessiv.A	Macro Virus
A97M.Amg.Trojan	Macro Virus
AM.Accessiv.A	Macro Virus
AM.Accessiv.B	Macro Virus
AM.Accessiv.C	Macro Virus
AM.Jaring.intended	Macro Virus
AM.Tox.A	Macro Virus
AM.Tox.B	Macro Virus

Current Files

	Creation Date
Virus Definitions	10/31/01
virscan1.dat	10/31/01

4276 virus names found

To export the virus list to a text file

1. In the Virus Definitions Info dialog box, click **Export**.
2. Specify where to save the file.
3. Open the exported text file in a word processing program to print it.

To search for a specific virus name

1. In the Virus Definitions Info dialog box, click **Search**.
2. In the Virus Name Contains field, type the name or part of the name of the virus.
3. Click **Find**.

Look up virus definitions on the Symantec Web site

Because of the large number of viruses, the Virus Definitions Info file does not include descriptions of each virus. The Symantec Security Response Web site contains a complete list of all known viruses and related malicious code, along with descriptions.

To look up virus definitions

1. Point your browser to the Symantec Security Response Web site at: http://securityresponse.symantec.com
2. Click the **Virus Encyclopedia** link.
3. Do one of the following:
   - Type a virus name for which to search.
   - Scroll through the alphabetical list to locate a virus.
4. Select a virus to read its description.

Customizing Norton AntiVirus for Macintosh

7

You can change Norton AntiVirus settings to fit your work environment.

For settings that govern the behavior of scanning, Norton AntiVirus Auto-Protect, and related activities, use the Preferences dialog box.

In Mac OS 8.1-9.x, the Tools menu has additional settings for the Scheduler and the Exceptions List. The Preferences menu has additional settings for Menu Security and Turn Auto-Protect Off.

Norton AntiVirus for Mac OS X v10.1 does not have a Tools menu, as the options contained on those menus do not apply.

About General Preferences

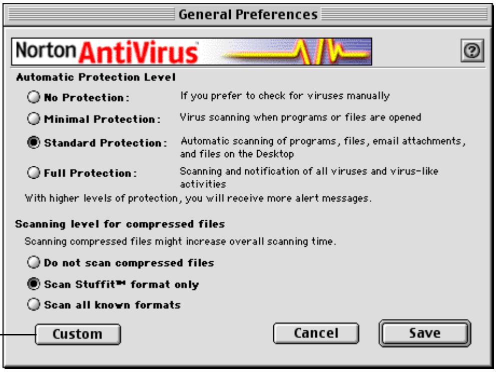
You can change the General Preferences that were set up when you installed Norton AntiVirus for Macintosh.

Set General Preferences in Mac OS 8.1–9.x

You can customize levels of prevention and compressed file scanning with the General Preferences dialog box. You can customize more features to a greater level of detail with the Custom Preferences dialog box.

To set Norton AntiVirus General Preferences

1 In the Norton AntiVirus main window, click **Preferences**.



General Preferences

Norton AntiVirus

Automatic Protection Level

○ **No Protection:** If you prefer to check for viruses manually

○ **Minimal Protection:** Virus scanning when programs or files are opened

● **Standard Protection:** Automatic scanning of programs, files, email attachments, and files on the Desktop

○ **Full Protection:** Scanning and notification of all viruses and virus-like activities

With higher levels of protection, you will receive more alert messages.

Scanning level for compressed files

Scanning compressed files might increase overall scanning time.

○ **Do not scan compressed files**

● **Scan Stuffit™ format only**

○ **Scan all known formats**

Opens Custom Preferences

2 If the Custom Preferences dialog box appears, click **General**.

3 Set the protection level.

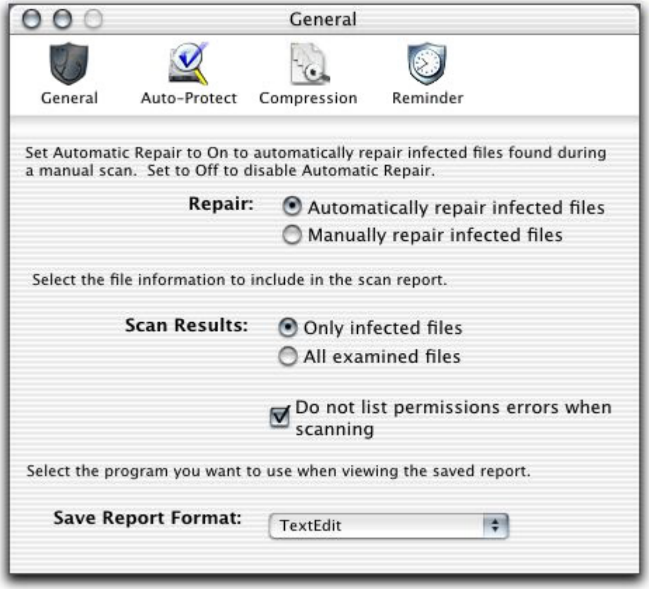
4 To customize Preference settings further, click **Custom**.
See "Access Custom Preferences in Mac OS 8.1-9.x" on page 90.

Set General Preferences in Mac OS X v10.1

Select your settings for Auto-Repair, Scan Results, and Save Report Format in the General Preferences window.

To set Norton AntiVirus General Preferences in Mac OS X v10.1

1 In the Norton AntiVirus main window, click **Preferences**.



Set Automatic Repair to On to automatically repair infected files found during a manual scan. Set to Off to disable Automatic Repair.

Repair: ● Automatically repair infected files
○ Manually repair infected files

Select the file information to include in the scan report.

Scan Results: ● Only infected files
○ All examined files

☑ Do not list permissions errors when scanning

Select the program you want to use when viewing the saved report.

Save Report Format: TextEdit

2 Select the preferences that you want. Your choices are:

Repair	Determines the action that Norton AntiVirus performs when it encounters a virus during a scan. You can choose to have Norton AntiVirus repair the infected file automatically or report the infected file without repairing it.
Scan Results	Determines what appears on the Scan History report. You can have only files with problems appear on the report, or all scanned files. (When All examined files is selected, scanning takes more time.)
Do not list permissions errors when scanning	In Mac OS X v10.1, Norton AntiVirus can scan only those files to which you have access permission. If this option is not selected, Norton AntiVirus lists each file it could not scan because it was denied access.
Report Format	Application that defines the format in which you want reports saved.

3 Close the window to save your changes.

About Custom Preferences

You can change a wide range of settings for the way Norton AntiVirus Auto-Protect and the Norton AntiVirus program behave.

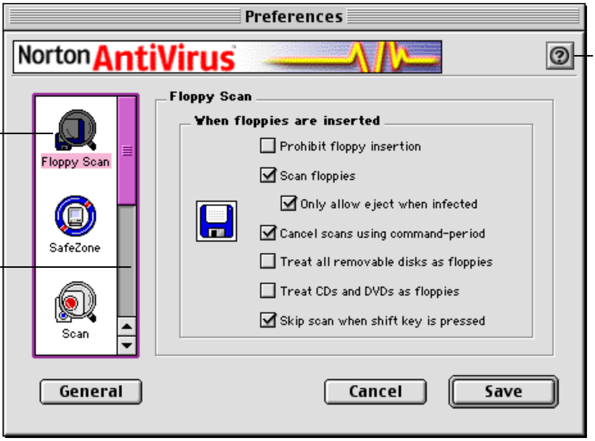
Access Custom Preferences in Mac OS 8.1–9.x

The Custom Preferences dialog box lets you configure scanning, Auto-Protect behavior, removable media scanning, alert types, SafeZone areas, virus-like activities, compression file types, and report file types. The left side of the Preferences dialog box contains sets of options that you can customize.

To access Custom Preferences

1 In the Norton AntiVirus main window, click **Preferences**.

2 If the General Preferences dialog box appears, click **Custom**.



Floppy Scan

When floppies are inserted

☐ Prohibit floppy insertion

☑ Scan floppies

☑ Only allow eject when infected

☑ Cancel scans using command-period

☐ Treat all removable disks as floppies

☐ Treat CDs and DVDs as floppies

☑ Skip scan when shift key is pressed

Select an icon in the list

Scroll to view more Preferences icons

Select to open Apple Guide help for Preferences

3 In the Custom dialog box, select an icon.

Floppy Scan	Determines how Norton AntiVirus Auto-Protect handles floppy disks and other removable media. See "About Floppy Scan Preferences" on page 92.
SafeZone	Determines what areas of your computer are protected by Auto-Protect. See "About SafeZone Preferences" on page 93.
Scan	Determines how Auto-Protect and the Norton AntiVirus program perform scans, and whether Auto-Protect alerts you to changes in program files. See "About Scan Preferences" on page 95.
Prevention	Customizes how Auto-Protect monitors virus-like activities. See "About Prevention Preferences" on page 98.
Alert	Customizes the types and durations of Auto-Protect alert messages. See "About Alert Preferences" on page 101.
Report	Identifies a file format for Activity Logs, and chooses which activities to record in the log. See "About Report Preferences" on page 103.
Compression	Chooses which types of compressed files you want to scan. See "About Compression Preferences" on page 105.

4 Make the changes to the Preferences settings.

5 Click **Save** when you are done.

Access Custom Preferences in Mac OS X v10.1

The Preferences dialog box contains three additional panes used to customize Norton AntiVirus. You can specify how you want Auto-Protect to run. You can choose the types of compression files you want Norton AntiVirus to scan. And you can set Norton AntiVirus to send you a notice when your virus definitions are out of date.

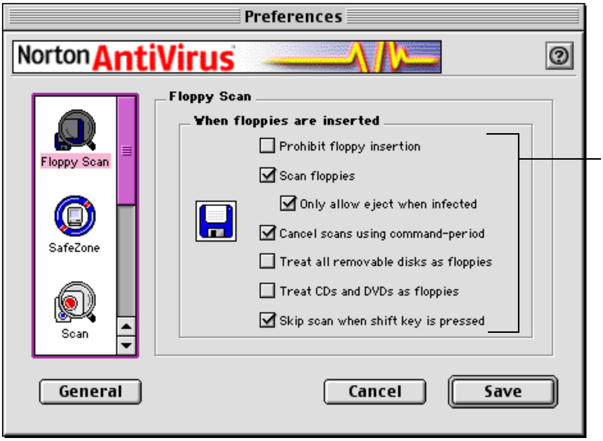
About Floppy Scan Preferences

A common way for a virus to enter your computer is through floppy disks or other removable media. To prevent this from happening, Auto-Protect scans these items each time they are inserted into your computer.

In Mac OS X v10.1, when Auto-Protect is on, all files on Hierarchical File System (HFS) Standard and HFS Plus Extended disks (which are all standard Mac-formatted disks) are scanned when they are created or modified. This also applies to removable media when they are mounted, if they are HFS or HFS Plus formatted.

To set Floppy Scan Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **Floppy Scan** icon.



Floppy Scan

When floppies are inserted

☐ Prohibit floppy insertion

☑ Scan floppies

☑ Only allow eject when infected

☑ Cancel scans using command-period

☐ Treat all removable disks as floppies

☐ Treat CDs and DVDs as floppies

☑ Skip scan when shift key is pressed

Customize floppy disk scanning

2 Specify the action that Norton AntiVirus should perform when a floppy disk is inserted. Your choices are:

Prohibit floppy insertion	Ejects all floppy disks. Norton AntiVirus does not allow access to floppy disks. This option must be unchecked to repair an infected floppy disk. If Treat all removable disks as floppies is also checked, all removable media is ejected.
Scan floppies	Scans floppy disks each time that they are inserted.
Only allow eject when infected	Automatically ejects floppy disks that contain infected files.
Cancel scans using command-period	Lets you stop an in-progress floppy disk scan.
Treat all removable disks as floppies	Causes all removable media, such as Jaz and Zip cartridges, to be scanned the same way as floppy disks.
Treat CDs and DVDs as floppies	Causes all nonwritable media to be treated like floppy disks.
Skip scan when Shift key is pressed	Lets you skip a floppy scan by pressing Shift while inserting a floppy disk.

3 Click **Save**.

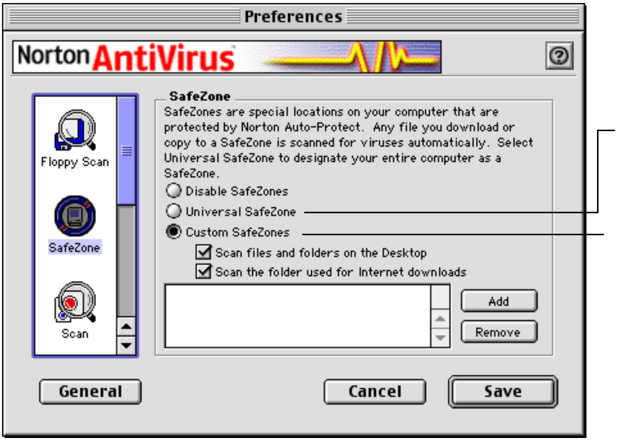
About SafeZone Preferences

In Mac OS 8.1-9.x, you can set up as many SafeZones on your computer as you need. You can also use the SafeZone Preferences to specify certain Auto-Protect scanning behaviors.

In Mac OS X v10.1, your entire computer is considered a Universal SafeZone and as such, no customizing is needed.

To Set SafeZone Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **SafeZone** icon.



SafeZone

SafeZones are special locations on your computer that are protected by Norton Auto-Protect. Any file you download or copy to a SafeZone is scanned for viruses automatically. Select Universal SafeZone to designate your entire computer as a SafeZone.

○ Disable SafeZones
○ Universal SafeZone
● Custom SafeZones
☑ Scan files and folders on the Desktop
☑ Scan the folder used for Internet downloads

Select to make the desktop a SafeZone

Select to designate additional folders as SafeZones

2 Specify the SafeZone settings. Your choices are:

Disable SafeZones	Prevents Norton AntiVirus Auto-Protect from automatically scanning any files that are created, downloaded, or moved.
Universal SafeZone	Causes Norton AntiVirus Auto-Protect to scan every file that is downloaded in addition to files that are created anywhere on the computer.
Custom SafeZones	Lets you specify additional folders as SafeZones.
Scan files and folders on the Desktop	Causes Norton AntiVirus Auto-Protect to scan all files and folders on your Desktop.
Scan the folder used for Internet downloads	Causes Norton AntiVirus Auto-Protect to automatically scan files when they appear in the folder designated for all Internet downloads. Specify this folder using the Internet Control Panel (on Mac OS 8.5 and later) or the Internet Config utility program (Mac OS 8 or 8.1).

3 Click **Save**.

Add and remove Custom SafeZones

You can add as many SafeZones as are appropriate for your work habits. When you no longer need a SafeZone, you can remove it.

To add a Custom SafeZone

1. In the SafeZone Preferences dialog box, click **Custom SafeZones**.
   By default, Scan files and folders on the Desktop is selected.
2. Click **Add**.
3. Select the folder or volume that you want to be a SafeZone.
   The location appears in the list.
4. Click **Save**.
   Auto-Protect will now scan the new SafeZones.

To remove a Custom SafeZone

1. In the SafeZone Preferences dialog box, click **Custom SafeZones**.
2. Select the SafeZone to be removed.
   If a Custom SafeZone volume is unavailable, it is listed as Not found.
3. Click **Remove**.
4. Click **Save**.

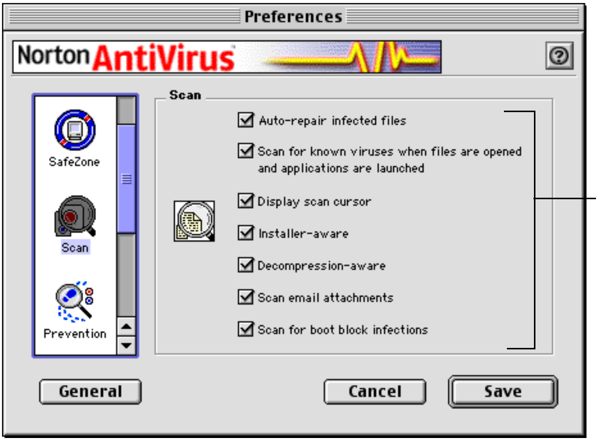
About Scan Preferences

In Mac OS 8.1-9.x, the Scan options apply to all scans performed by the Norton AntiVirus program and by Norton AntiVirus Auto-Protect. This includes scans you initiate, scheduled scans, automatic floppy disk scans, and scans that Norton AntiVirus initiates automatically (when you launch a program, for example).

! In Norton AntiVirus for Mac OS X v10.1, you can set preferences for scans performed by Auto-Protect. When removable media are mounted they are added to the volumes protected as part of a Universal SafeZone, and thus those files (formatted for HFS and HFS extended) are scanned and safe.

To Set Scan Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **Scan** icon.



Scan

☑ Auto-repair infected files

☑ Scan for known viruses when files are opened and applications are launched

☑ Display scan cursor

☑ Installer-aware

☑ Decompression-aware

☑ Scan email attachments

☑ Scan for boot block infections

Customize scanning options

2 Select the scan options that you want. Your choices are:

Auto-Repair infected files	Norton AntiVirus and Norton AntiVirus Auto-Protect automatically detect and repair infected files and inform you of the results.
Scan for known viruses when files are opened and programs are launched	Norton AntiVirus Auto-Protect scans programs when they are launched and scans documents when they are opened.
Display Scan cursor	The Scan cursor appears in place of the Macintosh pointer when Norton AntiVirus or Norton AntiVirus Auto-Protect are scanning files.
Installer-aware	Norton AntiVirus virus-like activity alerts are suppressed during installation of programs that use common installation programs.
Decompression-aware	Norton AntiVirus virus-like activity alerts are suppressed during decompression of compressed archives such as those created by StuffIt, Disk Doubler, Mac Binary, Zip and gzip, and other compression programs.

Scan email attachments	Norton AntiVirus Auto-Protect scans email attachments when they are downloaded. See "Scan email attachments" on page 67.
Scan for boot block infections	Norton AntiVirus scans the boot block for infections, and if configured, repairs them.

3 Click **Save**.

To set scanning preferences for Auto-Protect in Mac OS X v10.1

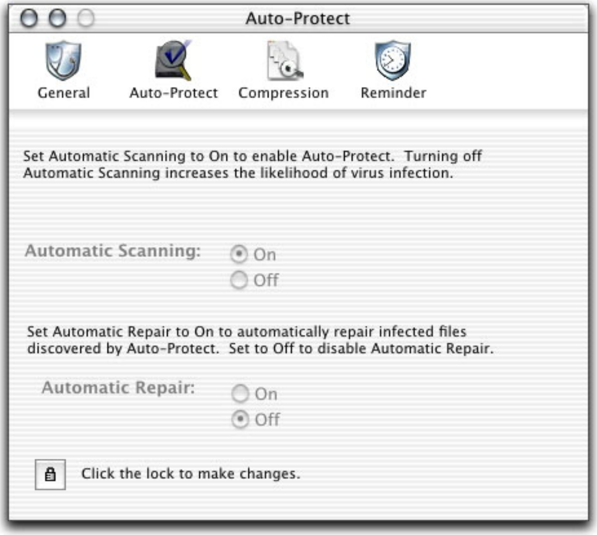
1 In the main Norton AntiVirus window, click **Preferences**.

2 In the General Preferences dialog box, click **Auto-Protect**.

3 In the Auto-Protect window, click **Click the lock to make changes**.

4 In the Authenticate dialog box, type your administrator name and password.

5 Click **OK**.
Select the automatic options that you want.



Set Automatic Scanning to On to enable Auto-Protect. Turning off Automatic Scanning increases the likelihood of virus infection.

Automatic Scanning: ● On ○ Off

Set Automatic Repair to On to automatically repair infected files discovered by Auto-Protect. Set to Off to disable Automatic Repair.

Automatic Repair: ○ On ● Off

Click the lock to make changes.

6 Close the window to save your changes.

About Prevention Preferences

In Mac OS X v10.1, virus-like activity is not monitored.

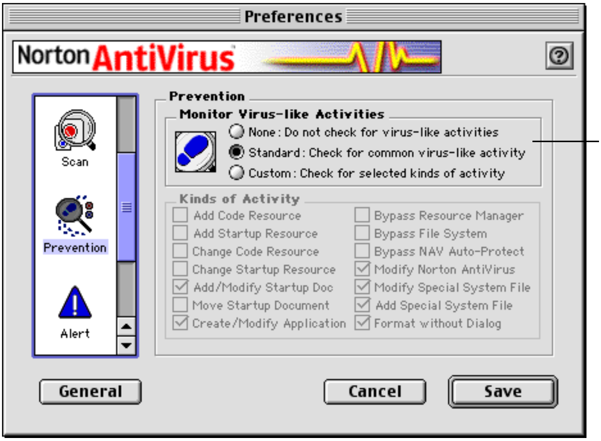
Use the Prevention options to set the level of virus-like activities monitored by Norton AntiVirus Auto-Protect. Although some programs perform these actions for valid reasons, Norton AntiVirus can monitor for these activities on the chance that an unknown virus is performing one of them. In most environments, the default Standard setting is sufficient.

See "If you receive a Virus-like Activity alert in Mac OS 8.1–9.x" on page 82.

If a virus-like activity is detected, it does not necessarily mean that a virus is performing the activity. You must decide whether to continue or not.

To set Prevention Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **Prevention** icon.



Prevention

Monitor Virus-like Activities

○ None : Do not check for virus-like activities
● Standard : Check for common virus-like activity
○ Custom : Check for selected kinds of activity

Kinds of Activity

☐ Add Code Resource
☐ Add Startup Resource
☐ Change Code Resource
☐ Change Startup Resource
☑ Add/Modify Startup Doc
☐ Move Startup Document
☑ Create/Modify Application
☐ Bypass Resource Manager
☐ Bypass File System
☐ Bypass NAV Auto-Protect
☑ Modify Norton AntiVirus
☑ Modify Special System File
☑ Add Special System File
☑ Format without Dialog

Select a prevention level for monitoring virus-like activity

2 Select a prevention level for monitoring virus-like activities.
If you select Custom, more activity types become active. Your choices are:

None	No virus-like activity monitoring.
Standard	Monitors programs for the most common virus behavior, such as adding code instructions to a program file. If you are not sure which option to choose, select Standard.
Custom	Lets you choose which virus-like activities Norton AntiVirus monitors.

3 Select the custom options that you want. Your choices are:

Add Code Resource	A program tries to add code instructions to another file. This is the most common way that viruses infect files.
Add Startup Resource	A program tries to add startup resource code to any file in the System folder. This is a common way viruses infect files.
Change Code Resource	A program tries to change a file's existing instructions. Programs rarely modify themselves. If this activity is detected, it can be an indication of a virus.
Change Startup Resource	A program tries to change code resources in a startup document. If this activity is detected, it may indicate a virus.
Add/Modify Startup Doc (default Standard option)	A program attempts to create a new startup document. Although this activity often happens legitimately (during the installation of new software, for example), it could indicate the presence of a virus.
Move Startup Document	A program tries to move a startup document into or out of the System folder. Although this activity often happens legitimately (when you move startup documents using the Finder, for example), it could indicate the presence of a virus.
Create/Modify Application (default Standard option)	A program tries to create or modify a program file. Although this activity often happens legitimately (when you copy files using the Finder, for example), it could indicate the presence of a virus.
Bypass Resource Manager	A program attempts to modify a resource file without going through the Macintosh Resource Manager. Modifications to a resource file are common; however, they normally take place using the Resource Manager. Although this activity often happens legitimately (when you use a backup program, for example), it could indicate the presence of a virus.

Bypass File System	A program attempts to modify a disk without going through the Macintosh file system. Although this activity could indicate the presence of a virus, some programs (such as ResEdit and Macintosh Programmer's Workshop) bypass the file system as part of their normal processing.
Bypass NAV Auto-Protect	A program attempts to modify a resource file without passing through checkpoints that Norton Auto-Protect sets up for monitoring modification attempts. This alert is rare. If it appears, be suspicious because only a few programs (for example, THINK C, Pascal, ResEdit, and some fax programs) bypass Norton AntiVirus Auto-Protect legitimately. Check the Read Me file for the names of any other software programs that bypass Norton AntiVirus Auto-Protect.
Modify Norton AntiVirus (default Standard option)	A program attempts to make changes to Norton AntiVirus. If this activity is detected, it could indicate the presence of a virus.
Modify Special System File (default Standard option)	A program attempts to write to the debugger, disassembler, or System file in a System folder. If this activity is detected, it could indicate the presence of a virus.
Add Special System File (default Standard option)	A program attempts to move, rename, or create a debugger or disassembler file in a System folder. Attempts like this are infrequent and should be viewed suspiciously.
Format without Dialog (default Standard option)	A program attempts to format a disk without the standard format dialog box. This may be caused maliciously by a Trojan horse or legitimately by a program, such as a utility program attempting to create a disk partition. Attempts like this are infrequent and should be viewed suspiciously.

4 Click **Save**.

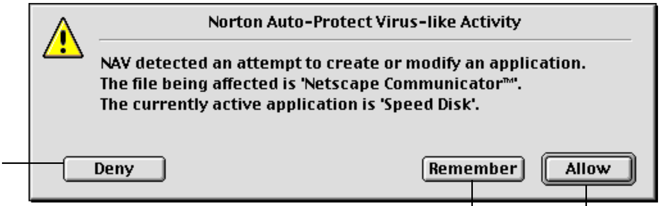
About Alert Preferences

In Mac OS X v10.1, modifying Alert Preferences is not available.

The Alert settings specify how Auto-Protect informs you that it has detected a virus or virus-like activity.

You can customize the message that appears in the alert dialog box, and change other characteristics of the alert. You can set how long the alert stays on the screen, enter a special message, alert others on a network, or set Auto-Protect not to alert you to this type of activity again.

Following is a typical virus-like activity alert in Mac OS 8.1-9.x.



Norton Auto-Protect Virus-like Activity

NAV detected an attempt to create or modify an application.
The file being affected is 'Netscape Communicator™'.
The currently active application is 'Speed Disk'.

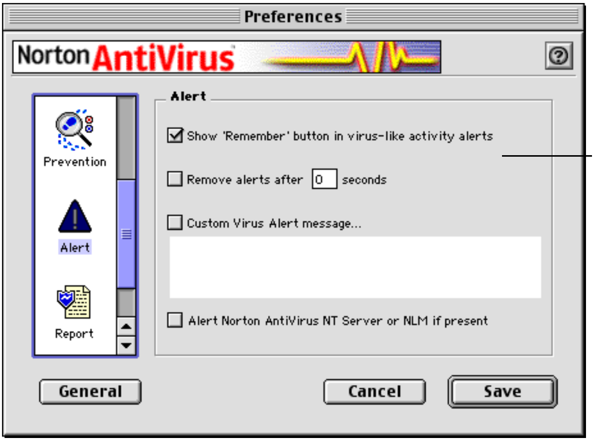
Prevents the virus-like activity from continuing

Allows the activity and doesn't display the alert next time

Allows the virus-like activity to continue with no further action

To set Alert Preferences in Mac OS 8.1-9.x

1 In the Preferences dialog box, click the **Alert** icon.



Preferences

Alert

☑ Show 'Remember' button in virus-like activity alerts

□ Remove alerts after 0 seconds

□ Custom Virus Alert message...

□ Alert Norton AntiVirus NT Server or NLM if present

Customize alerts

2 Select the options that you want.Your choices are:

Show Remember button in virus-like activity alerts	Select to have the Remember button appear in Virus-like activity alerts. Clicking Remember causes Norton AntiVirus Auto-Protect to ignore specific actions while a particular program is running. (This setting affects the Prevention preferences.) Sometimes Norton AntiVirus alerts you of actions that could be the work of a virus, but are not. In these cases, you can click Remember to add the file to the exceptions list, preventing the alert from appearing in the future. See "Manage virus-like activities" on page 109.
Remove alerts after seconds	Select to specify how long alert boxes stay on your screen before the default button is selected automatically. Type the number of seconds (0 to 99) in the seconds text box. For virus alerts, the default button is always Stop. For virus-like activity alerts the default button is always Allow. Uncheck this option if you want alerts to stay on the screen until you respond to them.
Custom Virus Alert message	Select if you want a custom message to appear in virus alerts and virus-like activity alerts. Type the message (such as Call Help Desk - 55555) in the text box.
Alert Norton AntiVirus NT Server or NLM if present	Select to have alerts from Norton AntiVirus sent to the Norton AntiVirus for Windows NT (NAV NT) Server or the Norton AntiVirus NetWare Loadable Module (NAVNLM) if it is present on your local network.

3 Click **Save**.

About Report Preferences

Norton AntiVirus generates three types of reports:

View History	Lists all the scans performed by Norton AntiVirus.
Norton AntiVirus main window	Lists scan results from scans that you initiate or schedule. You can print this information from the main window when a scan is completed.
Activity Log	Lists scan results from Norton AntiVirus Auto-Protect activity such as automatic floppy disk scans, automatic scans when documents are opened and when you launch a program, and virus-like activity alerts.

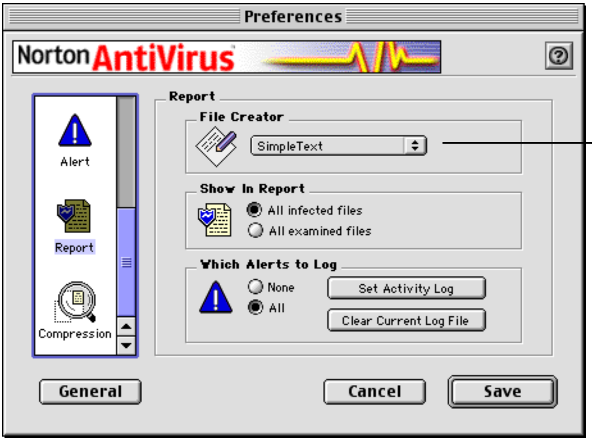
You can specify whether to have Norton AntiVirus generate reports on all files scanned, or only those with problems. You can also specify which program you use to view the saved scan report files.

For the Activity Log, you can specify its name and location and the types of alerts it records. You can also clear the Activity Log when it gets too big.

In Mac OS X v10.1, set the report file type on the General Preferences tab. See "About General Preferences" on page 87.

To set Report Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **Report** icon.



Preferences

Report

File Creator: SimpleText

Show In Report
● All infected files
○ All examined files

Which Alerts to Log
○ None
● All

Select reporting options

2 In the File Creator list, select a program in which to view saved reports and the Activity Log in the program of your choice.
Select **Other** to choose a program other than those listed. A dialog box appears in which you identify the program.

3 In the Show in Report group box, select an option to specify the scope of reported information when scans are performed. Your options are:

All infected files	Lists infected files only.
All examined files	Lists every scanned file and reports whether a problem was found or not. (When this option is selected, scanning may take longer on some computers.)

4 Select the Activity Log Preferences that you want.Your choices are:

Which Alerts to Log	Select an option to specify the type of alerts to save to the Activity Log.
None	Does not log any alerts in the Activity Log.
All	Logs virus warnings and virus-like activity alerts in the Activity Log.
Set Activity Log	Specifies a location for the Activity Log. You can also specify a different name for the file using this option. The default name is Norton AntiVirus Activity Log.
Clear Current Log File	Clears the contents of the Activity Log file.

5 Click **Save**.

View the Activity Log to see the results of your settings. The Activity Log contains the alerts you specified to log.

To view the Activity Log

1 In the Finder, locate the file.

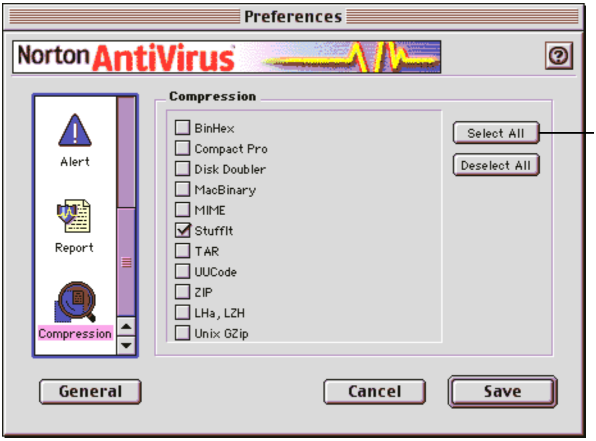
2 Double-click the file to open it in the program that you specified as the File Creator in the Report Preferences dialog box. The default program is SimpleText.

About Compression Preferences

Norton AntiVirus can scan different types of compressed files unless you changed the compression setting when installing. Norton AntiVirus automatically scans all StuffIt compressed files. In addition, Norton AntiVirus scans other types of compressed files using StuffIt technology from Aladdin Systems. You can specify which other compressed file types Norton AntiVirus should scan.

To set Compression Preferences in Mac OS 8.1–9.x

1 In the Preferences dialog box, click the **Compression** icon.



Compression

- ☐ BinHex
- ☐ Compact Pro
- ☐ Disk Doubler
- ☐ MacBinary
- ☐ MIME
- ☑ StuffIt
- ☐ TAR
- ☐ UUCode
- ☐ ZIP
- ☐ LHa, LZH
- ☐ Unix GZip

Select all compression types

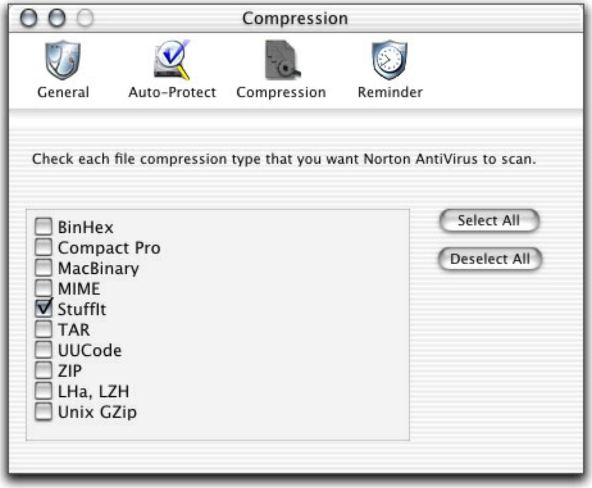
2 Do one of the following:

- Select the file compression types that you want Norton AntiVirus to scan.
- Click **Select All** to select all of the listed compressed file types.
- Click **Deselect All** if you do not want any compressed files to be scanned.
  Scanning time will be longer if you scan many compressed files.

3 Click **Save**.

To set Compression Preferences in Mac OS X v10.1

1 In the Preferences window, click **Compression**.



Check each file compression type that you want Norton AntiVirus to scan.

□ BinHex
□ Compact Pro
□ MacBinary
□ MIME
☑ StuffIt
□ TAR
□ UUCode
□ ZIP
□ LHa, LZH
□ Unix GZip

2 Do one of the following:

- Select the file compression types that you want Norton AntiVirus to scan.
- Click **Select All** to select all of the listed compressed file types.
- Click **Deselect All** if you do not want any compressed files to be scanned.
  Scanning time will be longer if you scan many compressed files.

3 Close the window to save your changes.

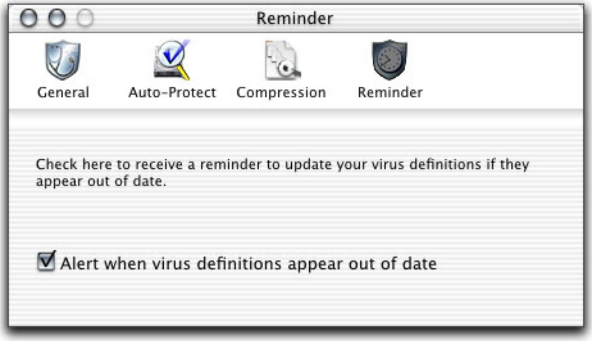
About Reminder Preferences

You can set Norton AntiVirus to notify you when your virus definitions are out of date. The latest virus definitions are necessary to keeping your computer virus-free.

In Mac OS 8.1-9.x, an automatic reminder is not available. Check your virus definitions manually using LiveUpdate. See “Keeping current with LiveUpdate” on page 49.

To set a reminder in Mac OS X v10.1

1 In the General Preferences window, click **Reminder**.



Check here to receive a reminder to update your virus definitions if they appear out of date.

☑ Alert when virus definitions appear out of date

2 Check **Alert when virus definitions appear out of date**.

3 Close the window to save your changes.

Password-protect Norton AntiVirus menus

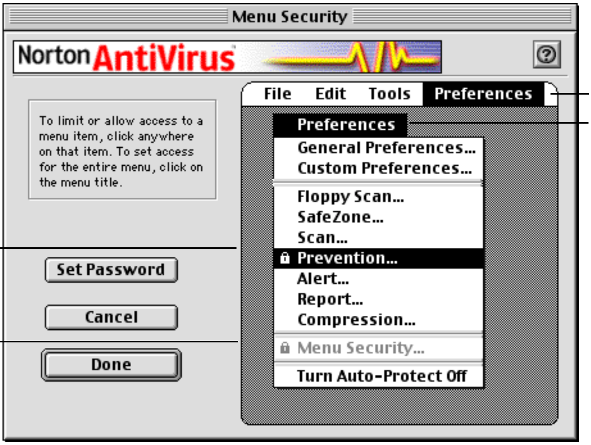
Menu Security is not available in Mac OS X v10.1.

You can restrict access to most settings by setting a password. Use the Menu Security command to define what features you want password-protected, and to set or change the password. After you assign a password, you must restart Norton AntiVirus before it becomes active.

If you assign a password to multiple menu items, unlocking one menu item will unlock them all for as long as Norton AntiVirus is running.

To password-protect Norton AntiVirus menus in Mac OS 8.1–9.x

1 On the Preferences menu, click **Menu Security**.



To limit or allow access to a menu item, click anywhere on that item. To set access for the entire menu, click on the menu title.

Select to display the menu contents

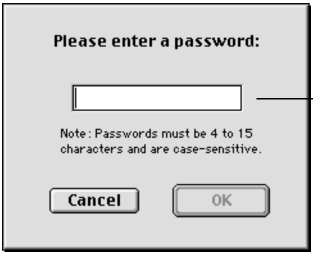
Select the title to protect the entire menu

Select a menu command to password-protect it

Dimmed items cannot be password-protected

2 To password-protect a specific menu command, select the menu command.

3 Click **Set Password**.



Please enter a password:

Note: Passwords must be 4 to 15 characters and are case-sensitive.

Type a password

4 Type a password between 4 and 15 characters long.
Passwords are case-sensitive. For example, a is not the same as A.

5 Click **OK**.

6 In the dialog box that appears, retype the password.

7 Click **OK**.

8 Click **Done**.
A padlock icon appears next to the protected features.

Change your password

Once you’ve established a password, you can change it.

To change your password

1. On the Preferences menu, click **Menu Security**.
2. Type your current password when prompted.
3. Click **Set Password**.
4. Type the new password.
5. Click **OK**.
6. In the dialog box that appears, retype the new password.
7. Click **OK**.
8. Click **Done**.

Remove password protection

If you no longer want password protection for some or all of the features you previously protected, you can remove the protection.

To remove password protection

1. On the Preferences menu, click **Menu Security**.
2. Type your password when prompted.
3. In the Menu Security dialog box, do one of the following:
   - Select the items that have a padlock icon next to them.
   - Click the menu title to unlock an entire menu.

   The padlock icon disappears.
4. Click **Done**.

Manage virus-like activities

The Exceptions List does not apply in Norton AntiVirus for Mac OS X v10.1.

You can edit the list of virus-like activities that you want Auto-Protect to ignore. The Exceptions List contains conditions or activities that would normally be flagged as virus-like, which you have told Auto-Protect to remember. This list also includes any decompression programs.

See “About Alert Preferences” on page 101.

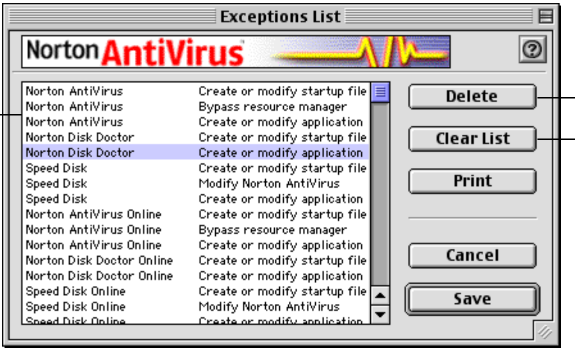
An Exception is saved when you click Remember in a virus-like activity alert. You can enable or disable this feature.

Remove entries from the Exceptions List

You can remove exceptions that you no longer want. For example, if you remove a program from your disk for which you had an exception, you can remove the exception saved for that program.

To remove entries from the Exceptions List

1 On the Tools menu, click **Edit Exceptions List**.



Norton AntiVirus	Create or modify startup file
Norton AntiVirus	Bypass resource manager
Norton AntiVirus	Create or modify application
Norton Disk Doctor	Create or modify startup file
Norton Disk Doctor	Create or modify application
Speed Disk	Create or modify startup file
Speed Disk	Modify Norton AntiVirus
Speed Disk	Create or modify application
Norton AntiVirus Online	Create or modify startup file
Norton AntiVirus Online	Bypass resource manager
Norton AntiVirus Online	Create or modify application
Norton Disk Doctor Online	Create or modify startup file
Norton Disk Doctor Online	Create or modify application
Speed Disk Online	Create or modify startup file
Speed Disk Online	Modify Norton AntiVirus
Speed Disk Online	Create or modify application

Applications and activities excluded from virus-like activity alerts

Deletes a selected item from the list

Deletes all exceptions from the list

2 In the Exceptions List dialog box, select the exceptions to delete.

3 Click **Delete**.

4 Click **Save** to save your changes.

Clear all entries from the Exceptions List

You can remove all entries from the Exceptions List. Be aware, however, that Norton AntiVirus Auto-Protect resumes alerting you of virus-like activities when they occur.

When you first install Norton AntiVirus, some exceptions are already set. These exceptions apply to standard behavior of various Symantec products, including Norton AntiVirus. If you clear all entries from the Exceptions List, you may receive virus-like activity alerts regarding these activities. You can add them back to the Exceptions List by clicking Remember in the virus-like activity alert.

To clear all entries from the Exceptions List

1. On the Tools menu, click **Edit Exceptions List**.
2. In the Exceptions dialog box, click **Clear List**.
3. Click **Save**.

Troubleshooting in Norton AntiVirus for Macintosh

8

See "Norton AntiVirus for Macintosh messages" on page 121.

The problems discussed in this chapter are not directly related to virus activity. If the problem you are trying to resolve is not in this chapter, consult the Read Me file on the Norton AntiVirus for Macintosh CD.

For a comprehensive list of the latest troubleshooting tips, see the Symantec Service and Support Web site, at this URL: www.symantec.com/techsupp/

Installation problems

See "Installing Norton AntiVirus for Macintosh" on page 19.

If you encounter any problems installing Norton AntiVirus, try restarting from the CD and installing Norton AntiVirus again.

My Macintosh continually starts from CD; I can't remove the CD

If your computer continues to start from the CD, use the Startup Disk Control Panel to reset the computer.

To restart your computer from the hard drive

1. In the Startup Disk Control Panel, make sure that your hard disk is selected.
2. On the Special menu, click **Restart**.
3. When you hear the startup chime, press the eject button on your CD-ROM drive to eject the CD.
   Your computer should now start from the hard disk.

I can't install Norton AntiVirus for Mac OS X v10.1

You must start your computer in Mac OS X v10.1 to run the Norton AntiVirus for Mac OS X v10.1 installer. And you must know your administrator password to install Norton AntiVirus.

Library file error message

If you experience problems with library files immediately after installing, you might still have incompatible files from a previous version of Norton AntiVirus for Macintosh. Delete the Norton AntiVirus Additions folder from the Extensions folder in your System Folder and reinstall Norton AntiVirus.

Startup problems

Startup problems could be due to problems with your computer, with Norton AntiVirus, or with settings you have made.

Norton AntiVirus Auto-Protect fails to load when I start my Macintosh

If Auto-Protect fails to load, any of several things could be the problem:

- Norton AntiVirus Auto-Protect may have a conflict with one or more of your other system extensions. Check the Norton AntiVirus Read Me file for the most up-to-date information on compatibility with other system extensions. If the Norton Read Me file does not provide the answer see "General Macintosh troubleshooting" on page 118.
- In Mac OS 8.1-9.x, if you are using an extension manager program, the program may have disabled Norton AntiVirus Auto-Protect. Start the extension manager program and make sure Norton AntiVirus Auto-Protect is enabled.
- Your copy of Norton AntiVirus Auto-Protect could be damaged in some way. In Mac OS 8.1-9.x, reinstall Norton AntiVirus Auto-Protect using the Custom install option.
- Make sure all engine files and virus definitions are installed. Norton AntiVirus does not run without them. For a list of all the installed files, see the NAV Install Log File located on the root of your hard disk.

Norton AntiVirus reports that a file is invalid when trying to launch or scan, or at startup

This is an indication that one of the files making up the virus definitions is damaged or otherwise invalid.

To repair a damaged virus definitions file in Mac OS 8.1-9.x

1. Open the System folder on your computer.
2. Find the Extensions folder and open it.
3. Open the Norton AntiVirus Additions folder.
4. Drag all of its contents to the Trash.
5. Reinstall Norton AntiVirus.
6. Run LiveUpdate and update your virus definitions.
   This restores the current versions of the items in the Norton AntiVirus Additions folder.

See "Installation" on page 23.

To repair a damaged virus definitions file in Mac OS X v10.1

1. Uninstall Norton AntiVirus.
2. Reinstall Norton AntiVirus.
3. Run LiveUpdate and update your virus definitions.
   This restores the current versions of the items in the Norton AntiVirus Additions folder.

See "Installation" on page 23.

Norton AntiVirus cannot find the Norton AntiVirus Virus Definitions file

Reinstall Norton AntiVirus.

Norton AntiVirus for Mac OS 8.1-9.x is password-protected and I forgot my password

Uninstall, then reinstall Norton AntiVirus.

In Mac OS 8.1-9.x, how do I prevent Norton AntiVirus from loading first?

Use an extension manager program to change the load order. Items in the Extensions folder load earlier than items in other locations in the System Folder.

Extensions load alphabetically, so changing the first character of the name is another way to change the load order. By changing the name of Norton AntiVirus Auto-Protect, you can change its location in the Control Panels folder of the System folder.

Why can't I create an alias to Norton AntiVirus?

If you did not install Norton AntiVirus, you cannot create an *alias* (a shortcut icon that points to an original object such as a file, folder, or disk) to it because of the access permissions established in Mac OS X v10.1. Have the person who installed the software create an alias and place the alias in an area to which you have access. You can then drag the alias to the location you want.

Protection problems

A file on the disk may be damaged, or Norton AntiVirus ran out of memory, or some other error occurred during scanning.

To determine if a file is causing the problem

See "How to start and exit Norton AntiVirus" on page 39.

1 Start Norton AntiVirus.

2 On the File View tab, click the drive triangle to display the folders inside.

3 Scan the folders one at a time to determine where the problem is occurring.

4 Scan your disk again from the Norton AntiVirus main window. You may also want to examine the disk using a program such as Norton Disk Doctor (part of Norton Utilities for Macintosh).

In Mac OS 8.1-9.x, if you have large files, or a large number of files, you may need to raise the memory allocation for Norton AntiVirus.

To increase memory allocation in Mac OS 8.1–9.x

1 Close Norton AntiVirus.

2 Select the **Norton AntiVirus** icon.

3 On the File menu, click **Get Info**.

4 Increase the memory allocation in the Preferred Size field.

In Mac OS X v10.1, Norton AntiVirus scans only those files for which your account has access privileges. You can do one of three things:

- If you ever log on and work as root, run the scan while logged on as root.
- If you do not log on as root, running the scan while logged on as an Administrator scans all files that could be infected while using that logon. If you do not want to see the list of files that could not be scanned because of denied access, check Do not list permissions errors when scanning in Preferences.
- Restart your computer from the Norton AntiVirus for Macintosh CD and scan your computer using Norton AntiVirus for Mac OS 8.1-9.x to avoid access problems.

I need to rescan files that have already been scanned

The Norton AntiVirus QuickScan file records whether you have already scanned a file using the currently installed virus definitions and libraries. If not, the file is scanned. If you want all files to be scanned regardless, you can use Norton AntiVirus to delete the QuickScan file at the root of each disk. The file is named NAV• 7.0 QuickScan in Mac OS 8.1-9.x and NAV• Mac800QSFile in Mac OS X v10.1.

To remove the QuickScan file

1. In the Norton AntiVirus window, on the File View tab, ensure that Show Invisible Files is checked.
2. Select your hard disk.
3. Click the **QuickScan** file.
   If there are QuickScan files from previous versions of Norton AntiVirus, select them as well.
4. Click **Move To Trash**.
5. Click **OK**.
6. Quit Norton AntiVirus.
7. In the Finder, click **Empty Trash**.

After you have deleted the QuickScan file, the first scan with the new virus definitions will be slower.

I'm having trouble updating virus definitions using LiveUpdate

In some rare cases such as immediately after the emergence of a new virus, the LiveUpdate servers may be very busy and it may be difficult to get a connection. In such cases, keep making connection attempts and you should eventually be successful.

When using LiveUpdate, make sure your Internet connection is working by testing the connection with your application, such as your Web browser.

General Macintosh troubleshooting

In Mac OS 8.1-9.x, if you experience a problem starting your Macintosh after installing Norton AntiVirus, there may be a conflict with other extensions on your computer. Follow the procedures below to troubleshoot the problem.

You should try restarting your computer with Extensions disabled. Extensions may conflict for one or more of the following reasons:

- There may be more than one copy of the System file on the same partition.
- A file may be damaged.
- The files may need to be loaded in a different order.
- One of the files may need to be updated.

Other troubleshooting steps

Here are some other steps you can take to resolve problems with your Macintosh.

- Reinstall or upgrade the System software.
  For more information, see your Macintosh System documentation.
- Use Norton Utilities for Macintosh to find and fix disk problems.
- Rebuild the Desktop file.
  For more information, see your Macintosh System documentation.
- Reinstall Norton AntiVirus.

See "Installing Norton AntiVirus for Macintosh" on page 19.

- Update the disk driver.
  For more information, see your Macintosh System documentation.
- Reset the PRAM (Parameter RAM).
  For more information, see your Macintosh System documentation, or the Norton Utilities for Macintosh documentation.

Norton AntiVirus for Macintosh messages

A

The following messages might be encountered when you are running Norton AntiVirus or Norton AntiVirus Auto-Protect.

Angle brackets (<>) identify variables or file names.

Mac OS 8.1–9.x and Mac OS X v10.1 messages

The entered subscription code is not valid. Please retype in the 9 character subscription code again.

You entered a virus definitions subscription code incorrectly. Try typing the number again.

The passwords did not match. Please try again.

The second password you typed does not match the first one.

That password is incorrect. Please try again.

You typed an incorrect password. If you forgot your password, see "Troubleshooting in Norton AntiVirus for Macintosh" on page 113.

The software to be installed requires Administrator or higher level access privileges.

Enter your administrator password.

There is not enough memory to view any more items. Collapse some of the expanded items and try again.
No more items can be viewed: <error string>. Collapse some of the expanded items and try again.

See "General Macintosh troubleshooting" on page 118.

There is not enough available memory for Norton AntiVirus to display or store information for the number or the size of files on the disks to be scanned. Try collapsing folders, scanning a more limited area, or changing the memory allocated to Norton AntiVirus in the Finder. Also, set Report Preferences to show only infected files.

The startup disk is read-only. Preferences can be changed, but will not be saved when you quit.

If you restarted from the CD-ROM and changed Norton AntiVirus preferences, they apply to the current session, but are not saved to the active System Folder on the CD. To change and save preferences to your System Folder, you must install Norton AntiVirus on your hard disk.

The item(s) you have selected to scan contain too many files to scan with report all examined items on. There is not enough memory to display all examined items. You can continue scanning with report all examined items turned off.

See "About Report Preferences" on page 103, and "General Macintosh troubleshooting" on page 118.

The setting in Report Preferences should be changed to All Infected Files. You could also try scanning a more limited area, or changing the memory allocated to Norton AntiVirus in the Finder.

The "Event Type" option has been changed to "Scan System disk" because only the System disk or folder can be scanned at startup.

The startup scan you scheduled can only scan the System Folder or the entire system disk.

The "How often" option has been changed to "weekly" because "always" can only be used with startup or shutdown scans.

When you change the type of scan from startup or shutdown to some other type, the frequency must also change if it was set to always. The always setting only applies to startup and shutdown scans.

The "When" option has been changed to "at specified time" because virus definition updates cannot be scheduled at startup or shutdown.

Virus definitions updates cannot occur at startup or shutdown. You must specify a different time for the update to occur.

The “Start Time” for the displayed event can't be saved until a valid number is entered in the <“minute”>, <“hour”>, or <“day”>, <“month”>, or <“year”> field.

In the Scheduler, make sure you enter a valid date and time for the event you are scheduling.

The scheduled events could not be saved because an error occurred: <error string>

Try deleting the Norton Schedule File (located in the Preferences folder within the System folder) and rescheduling the event.

There is no printer selected in the Chooser, or the selected printer could not be found.

You can’t print the Activity Log or scan report because your printer could not be found. Reselect the printer in the Chooser and try again.

There is not enough memory to add any more items to the scan report. You can continue scanning but non-infected items will be removed from the scan report and will not be added as the scan continues.

Norton AntiVirus uses available memory to store items for the scan report. If you have many files, you will not be able to record all items to scan. You can change the Report Preferences to record infected files only.

Mac OS 8.1–9.x specific messages

Norton AntiVirus could not locate the “Norton AntiVirus Macro Scan Lib” in the “Norton AntiVirus Additions” folder. It is required to scan for macro viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

A network error occurred that will prevent Norton AntiVirus from alerting the Norton AntiVirus NT or NLM Server when a virus is found. You can continue, but any viruses identified will not be reported to a network server.

If you want to alert others on the network, save the scan report and send it separately. Also, make sure that you are on the network.

Norton AntiVirus could not locate “Norton AntiVirus Library” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

Norton AntiVirus could not locate the “Norton AntiVirus Virus Defs” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

An error occurred loading the “Norton AntiVirus Library.” It is required to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

Mac OS X v10.1 specific messages

Norton AntiVirus could not locate the “Norton AntiVirus Virus Defs” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the /library/Application Support/Norton Solutions Support/Norton AntiVirus/Engine. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

An error occurred loading the “Norton AntiVirus Library.” It is required to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the /library/Application Support/Norton Solutions Support/Norton AntiVirus/Engine. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

Auto-Protect messages

Norton AntiVirus Auto-Protect is damaged. It may be infected with a virus!

Scan all volumes with Norton AntiVirus from a CD or locked floppy, then reinstall Auto-Protect.

The Norton AntiVirus Virus Defs file could not be loaded. Either the file is not in the Norton AntiVirus Additions folder, or it is invalid.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

The Norton AntiVirus Activity Data file was not found in Norton AntiVirus Additions or it is damaged.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

The Macro Scan Library could not be found, but Auto-Protect will still perform its other functions.

Norton AntiVirus Auto-Protect is searching for a required file. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

The Norton AntiVirus Library could not be found in Norton AntiVirus Additions or it is damaged.

Norton AntiVirus Auto-Protect is searching for a required file. For more information, see the NAV Install Log File located on the root of your hard disk.

There was a problem with the Norton AntiVirus Preferences file.

Norton AntiVirus Auto-Protect is searching for the Preferences file, or the file may be damaged. Try deleting the file.

A PowerPC processor is required.

Norton AntiVirus must have a PowerPC processor to run.

Auto-Protect messages specific to Mac OS 8.1-9.x

Norton AntiVirus Auto-Protect requires the shared library <xxxx>.

Norton AntiVirus Auto-Protect is searching for a required file. For more information, see the NAV Install Log File located on the root of your hard disk. Try reinstalling Norton AntiVirus.

Norton AntiVirus Auto-Protect was not loaded because

One of the following appears at the end of the message:

- Norton AntiVirus Auto-Protect did not have enough memory.
  - Norton AntiVirus Auto-Protect is already loaded.
  - System 8.1 or Power Macintosh is required.

Auto-Protect messages specific to Mac OS X v10.1

Norton AntiVirus Auto-Protect could not continue. Please reinstall Norton AntiVirus and restart.

One of the files in /library/Application Support/Norton Solutions Support/Norton AntiVirus/Engine is missing or damaged. Reinstall.

Using AppleScript with Norton AntiVirus

B

Norton AntiVirus for Macintosh lets you use your AppleScript to run certain features. To use this scriptable component, you must write an AppleScript script. Information on creating scripts is available on your Macintosh OS CD. AppleScript is not supported by Symantec Technical Support.

Scripting is not available on Norton AntiVirus for Mac OS X v10.1. However, the Command Line Scanner can be called with UNIX shell scripts.

Script commands

The following commands are available for use with Norton AntiVirus for Macintosh:

Script command	Description
scan	Scan the given files and folders for viruses.
load antivirus	Load the Norton AntiVirus Library and Norton AntiVirus Macro Scan Lib.
unload antivirus	Unload the Norton AntiVirus Library and the Norton AntiVirus Macro Scan Library.
get file of	Extract the file object from a report object.
get viruses of	Get the list of viruses that infect the file of the report.

Script command	Description
get repaired status of	Get the status of the repair from a given report.
Class scan result	The result of a scan, including the total number of files scanned, and the reports of all irregular (damaged or infected) files.

Within the scripting, you can cause Norton AntiVirus for Macintosh to display or hide its progress during scans. The script-initiated scan results, including the discovery and repair of infected files, can be saved in a text file. The Norton AntiVirus for Macintosh scriptable component does not handle compressed files.

C

Using Norton AntiVirus on a network

You can run Norton AntiVirus on any AppleTalk Transaction Protocol server such as AppleShare or TOPS. You can configure Norton AntiVirus to alert you or others on the network if a virus is found on a client computer running Norton AntiVirus NetWare Loadable Module (NAV NLM) or Norton AntiVirus for Windows NT (NAV NT). This appendix offers tips and suggestions for using Norton AntiVirus efficiently on a network.

Notes to the administrator

Set up Norton AntiVirus the following way in a networking environment:

- Run Norton AntiVirus Auto-Protect and the Norton AntiVirus application on the system administrator’s computer.
    - Make sure Norton AntiVirus Auto-Protect is run on all workstation Macintosh computers.
    - Use the Scheduler command from the Norton AntiVirus Tools menu to schedule periodic scans of all network drives.

Scanning network drives

When you are scanning network drives from a workstation, the server slows down for other users. If others are creating, deleting, or moving files on a network drive while Norton AntiVirus is scanning, all files may not get scanned.

To prevent files from not getting scanned, do the following:

- Make sure that you are the only one logged on to the server when scanning network drives.
- Shut down the server and restart it from the Norton AntiVirus for Macintosh CD, then perform the scan.

Using Norton AntiVirus Auto-Protect on a server

Use Norton AntiVirus Auto-Protect on your network servers to protect against viruses. Norton AntiVirus Auto-Protect monitors file activity and alerts you if a virus tries to infect any applications on the server.

In Mac OS 8.1-9.x, if you are using the Prevention feature to monitor virus-like activities, you may experience delays because Norton AntiVirus Auto-Protect constantly monitors the Macintosh on which it is installed.

To prevent a network slowdown when Prevention features are active

1. In the Norton AntiVirus main window, click **Preferences**.
2. In the Prevention Preferences, click **Standard**.
   The Standard option monitors applications for the most common virus behavior, such as adding code instructions to an application file.
3. In the Alert Preferences, click **Remove alerts after**.
4. In the seconds text box, type **0**.
   This causes Norton AntiVirus Auto-Protect to accept the default button in the alert box, and prevents virus-like activity alerts from preventing access to files on the server.
5. In the Report Preferences, under Which Alerts To Log, click **All**.
   This ensures that virus-like alerts are logged in the Activity Log so that you can view the alerts at a later time.

See "About Prevention Preferences" on page 98.

See "About Alert Preferences" on page 101.

Preparing an emergency response plan

To be fully prepared in case of a virus attack on a workstation, be sure to have a detailed emergency response plan written and distributed within your networking group before a problem arises. This maintains order and prevents panic in case of an infection.

The following sections include a partial listing of the items that should be included in your plan. Complete your plan based on the dynamics and needs of your organization.

Before a virus is detected

Conduct an informational meeting with your network users to discuss the basic nature and behavior of computer viruses. Stress that while having a computer virus on your system is reason to take immediate action, there is no need to panic. Emphasize that many viruses spread from illegal software copies, and prohibit the use of such software in your organization. Finally, explain how you've configured Norton AntiVirus to respond to a virus.

See "About Alert Preferences" on page 101.

In Mac OS 8.1-9.x, you can add a customized message to all virus alerts and virus-like activity alerts to indicate who the user should call for help (for example, "Call Help Desk for help at ext. 5555").

Instruct your users to:

- Scan all software before using it. This includes programs downloaded from the Internet as well as new software.
- Watch for warning signs such as frequent system crashes, lost data, screen interference, or suddenly unreliable programs.
- Keep a current store of virus-free program backups.
- Avoid running programs from unscanned removable media.
- Write-protect removable media before using it in someone else's computer.

To protect the workstations:

- Scan each workstation to make sure that it is virus-free.
- Train your users to use a file backup utility on a regular basis.
- Train your users to update the virus definitions file when it becomes available.

To protect the network:

- Password-protect all network executable directories so that only the administrator has write access to them.
- Scan for viruses on new and rented computers before using them.
- Schedule periodic scans of all network servers.
- If you are using Novell NetWare or Windows NT servers, use Norton AntiVirus Enterprise Solution components to protect servers from virus infections.

See "Service and support solutions" on page 133.

If a virus is detected

If a virus is detected on your network, remove it from all computers attached to the network.

To remove a virus

1. Physically disconnect the workstation from the network.
2. Eradicate the virus on the workstation before reconnecting to the network.
3. Notify other users on the network to scan for viruses immediately.
4. Scan your network servers for viruses.
5. In Mac OS 8.1-9.x, set Norton AntiVirus Preferences to alert you over a network running under Norton AntiVirus NetWare Loadable Module (NAV NLM) or Norton AntiVirus for Windows NT (NAV NT).

See "About Alert Preferences" on page 101.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.
- PriorityCare telephone support
  PriorityCare fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.
  You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.
- Automated fax retrieval
  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 726-9410.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for up to twelve months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at: http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Ring

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12 andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico Blvd Adolfo Ruiz Cortines, No. 3642 Piso 14 Col. Jardines del Pedregal Ciudad de México, D.F. C.P. 01900 México	http://www.service.symantec.com/mx +52 (5) 661-6120

Other Latin America

Symantec Corporation 9100 South Dadeland Blvd. Suite 1810 Miami, FL 33156 U.S.A.	http://www.service.symantec.com/mx

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

October 31, 2001

Glossary

administrator

1. A person who oversees the operation of a network. 2. A person responsible for installing programs on a network and configuring them for distribution to workstations. This person may also update security settings on workstations.

alert

A dialog box that appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.

alias

A shortcut icon that points to an original object such as a file, folder, or disk.

browser

A software application that makes navigating the Internet easy by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.

compressed file

A file that has been compressed using a special data storage format in order to save space on your disk.

compression

Using a mathematical algorithm to process data from a file or disk, such that the resulting data occupies less physical space on the disk. Individual files or entire disks can be compressed by various types of utility software.

document file

A file that is created by, or associated with, a program and contains no executable code. Examples include word processing documents, databases, and spreadsheets.

download

To transfer a file from one computer system to another, through a modem or network. Download usually refers to the act of transferring a file from the Internet, a BBS (bulletin board system), or a service such as America Online.

email (electronic mail) A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (HyperText Transfer Protocol) for sending and receiving email.

executable file A file containing program code that can be launched. Generally includes any file that is a program, extension, or a system file.

file type The four-character code, stored along with a creator code in each file, that identifies its type. Programs use this code to determine if a file is in a format that can be read by the program.

hard disk A device that reads data from, and writes data onto, a disk.

icon A graphic symbol used to represent a file, folder, disk, or other entity.

infected file A file that contains a virus.

Internet A decentralized global network connecting millions of computers.

known virus Any virus that Norton AntiVirus can detect and identify by name.

local A term that refers to your computer, as opposed to a remote computer.

network A set of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users.

operating system A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mice.

password A character sequence entered by users to verify their identities to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.

program

A set of instructions that can be executed by a computer, and are written for a specific purpose such as word processing or creating a spreadsheet. Also called software.

read-only

A disk, folder, or file containing data that can be read, but cannot be written to or deleted. Also referred to as locked or write-protected.

removable media

Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, disk cartridges (SyQuest and Bernoulli, for example), CDs, and Zip disks.

script

A list of instructions that can be executed without user interaction. Unlike other types of programs, scripts can be opened with text editors or word processing programs, so they are very easy to change. Examples of scripts include Visual Basic programs and network login scripts.

startup disk

A disk that contains the System files necessary to start your computer. Startup disk usually refers to a floppy disk or CD that can be used to start the computer in an emergency.

system extension

A program that loads into memory when a Macintosh computer is started. Also known as an INIT or startup document.

System file

The file stored in the System folder that the Macintosh computer uses to start up.

System folder

The folder on the startup disk that contains the files your Macintosh computer requires to run, such as the System file, Finder, system extensions, desk accessories, and control panels.

Trojan horse

A destructive program often designed to cause damage or do something malicious to a system, while disguised as something useful or interesting. Unlike viruses, Trojan horses don’t make copies of themselves. Some Trojan horse programs perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote-control capabilities for hackers.

unknown virus

A virus for which Norton AntiVirus does not contain a virus definition.

virus A self-replicating program intentionally written to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages. Self-replication differentiates viruses from other virus-like computer infections such as Trojan horse programs and worms.

virus definition Virus information that lets an anti-virus program recognize and alert you to the presence of a specific virus.

virus definitions file A file used by Norton AntiVirus to find and repair viruses. The virus definitions files must be updated regularly. LiveUpdate automates the process of downloading updated virus definitions files.

Virus List A list that shows all of the viruses for which Norton AntiVirus has a virus definition. It is important to update this list regularly.

virus-like activity An activity or action that Norton AntiVirus perceives as the work of a possible unknown virus. Virus-like activity alerts do not necessarily indicate the presence of a virus, but should be investigated.

Web page A single document on the World Wide Web that is identified by a unique URL. A Web page can contain text, hyperlinks, and graphics.

Web site A group of Web pages managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other Web pages.

worm A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down. So far, worms do not exist in the Macintosh world.

write-protect Write-protecting disks prevents viruses from infecting them. To write-protect a 3.5-inch disk, slide the tab on the back of the disk to uncover the hole through the disk. Also referred to as a locked disk or read-only disk.

Index

Norton AntiVirus™ for Macintosh®

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ______________________________

Company Name ______________________________

Street Address (No P.O. Boxes, Please) ______________________________

City ______________________________ State _______ Zip/Postal Code ______________

Country* ______________________________ Daytime Phone ______________________________

Software Purchase Date ______________________________

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem: ______________________________

CD Replacement Price	$ 10.00
Sales Tax (See Table)	
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).
Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ AMEX

Credit Card Number ______________________________ Expires __________

Name on Card (please print) ______________________________ Signature ______________________________

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

symantec™